Defense Information Systems Agency

A Combat Support Agency

VTF DIACAP Scorecard Matrix Instructions

DISN Video Services
October 2, 2009

DISA

A Combat Support Agency

How to Use the VTF DIACAP Scorecard Matrix

DISN Video Services (NS5)

DISA
A Combat Support Agency

Introduction

- **The VTF DIACAP Scorecard Matrix is the most efficient way to translate STIG test results into a completed DIACAP Scorecard for your Video Teleconferencing (VTC) information system (IS).**
- **You could conduct the STIG tests, fill in the Scorecard Matrix, and print out a copy of the Scorecard page of the Scorecard Matrix for your DAA to sign.**
- **Or, if you are using an automated tool like eMass, since the Scorecard Matrix summarizes compliance status with all applicable STIGs and 8500.2 IA controls, it makes a really good artifact that you can upload.**
- **The STIGs and the Scorecard Matrix can be used with the DIACAP Knowledge Service (KS) IA Control Validation Procedures.**
- **This presentation shows you how to use this unique tool.**

DISA
A Combat Support Agency

Presentation Outline

- **The following basic three-step demonstration shows you how to put STIG test results into the VTF DIACAP Scorecard Matrix.**
- **After the three steps, there are some important tips about the Scorecard Matrix.**
- **Next there are instructions on how to complete the Scorecard Matrix so it can automatically generate a DIACAP Scorecard for your IS.**

DISA
A Combat Support Agency

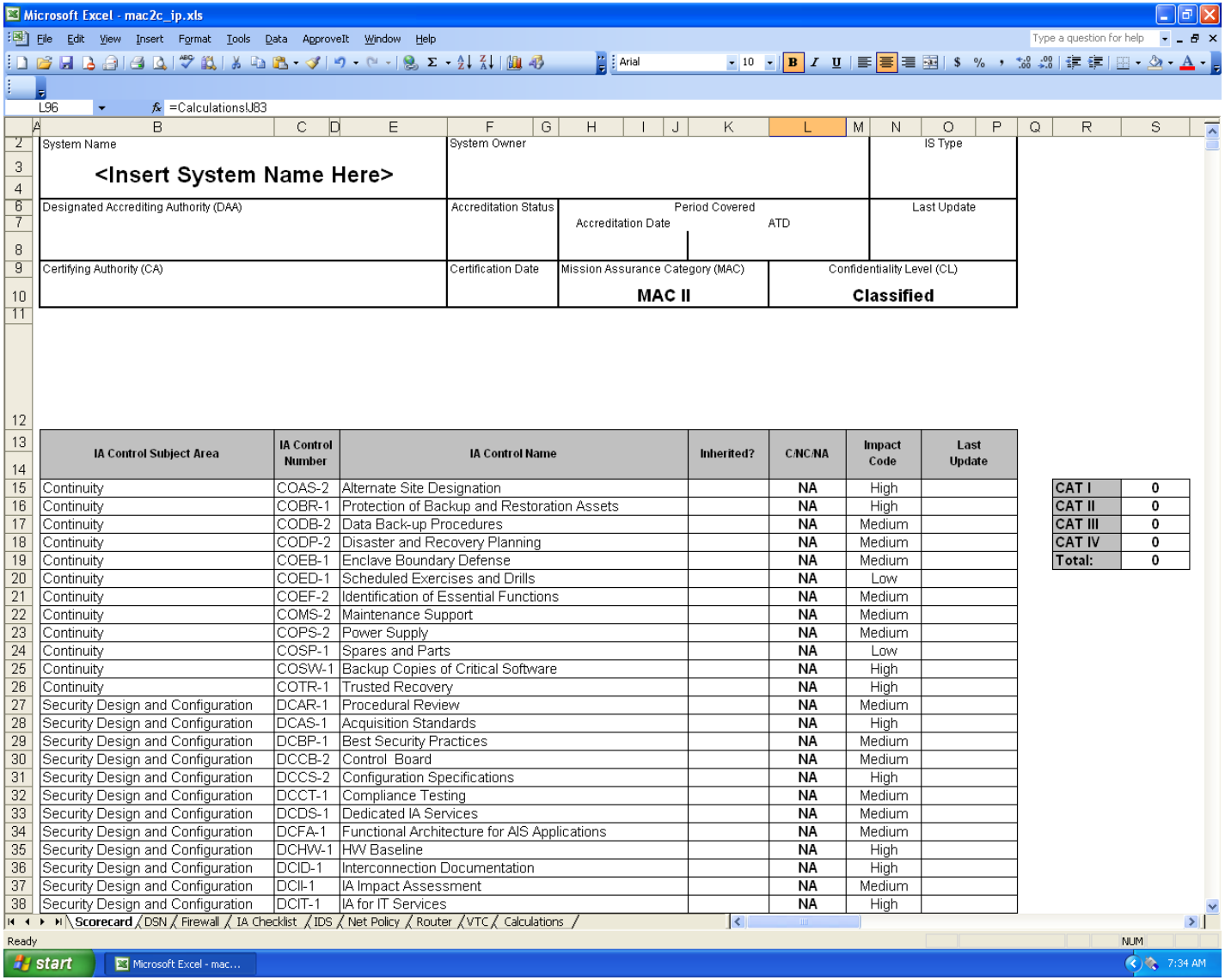
Step 1: Find the Correct Page

- There are several Scorecard Matrices.
  - Depend on Mission Assurance Category (MAC) and type of connectivity
    - ISDN and/or IP
- For this exercise, let's open the MAC II Classified Scorecard Matrix for IS that use ISDN and/or IP.

DISA

A Combat Support Agency

Step 1: Find the Correct Page


Microsoft Excel - mac2c_ip.xls
File Edit View Insert Format Tools Data ApproveIt Window Help
L96 =CalculationsU83
System Name
<Insert System Name Here>
System Owner
IS Type
Designated Accrediting Authority (DAA)
Accreditation Status
Period Covered
Accreditation Date
ATD
Last Update
Certifying Authority (CA)
Certification Date
Mission Assurance Category (MAC)
MAC II
Confidentiality Level (CL)
Classified
IA Control Subject Area | IA Control Number | IA Control Name | Inherited? | C/NC/NA | Impact Code | Last Update
Continuity | COAS-2 | Alternate Site Designation | NA | High
Continuity | COBR-1 | Protection of Backup and Restoration Assets | NA | High
Continuity | CODB-2 | Data Back-up Procedures | NA | Medium
Continuity | CODP-2 | Disaster and Recovery Planning | NA | Medium
Continuity | COEB-1 | Enclave Boundary Defense | NA | Medium
Continuity | COED-1 | Scheduled Exercises and Drills | NA | Low
Continuity | COEF-2 | Identification of Essential Functions | NA | Medium
Continuity | COMS-2 | Maintenance Support | NA | Medium
Continuity | COPS-2 | Power Supply | NA | Medium
Continuity | COSP-1 | Spares and Parts | NA | Low
Continuity | COSW-1 | Backup Copies of Critical Software | NA | High
Continuity | COTR-1 | Trusted Recovery | NA | High
Security Design and Configuration | DCAR-1 | Procedural Review | NA | Medium
Security Design and Configuration | DCAS-1 | Acquisition Standards | NA | High
Security Design and Configuration | DCBP-1 | Best Security Practices | NA | Medium
Security Design and Configuration | DCCB-2 | Control Board | NA | Medium
Security Design and Configuration | DCCS-2 | Configuration Specifications | NA | High
Security Design and Configuration | DCCT-1 | Compliance Testing | NA | Medium
Security Design and Configuration | DCDS-1 | Dedicated IA Services | NA | Medium
Security Design and Configuration | DCFA-1 | Functional Architecture for AIS Applications | NA | Medium
Security Design and Configuration | DCHW-1 | HW Baseline | NA | High
Security Design and Configuration | DCID-1 | Interconnection Documentation | NA | High
Security Design and Configuration | DCII-1 | IA Impact Assessment | NA | Medium
Security Design and Configuration | DCIT-1 | IA for IT Services | NA | High
CAT I 0
CAT II 0
CAT III 0
CAT IV 0
Total: 0
Scorecard DSN Firewall IA Checklist IDS Net Policy Router VTC Calculations
Ready
start
Microsoft Excel - mac...
7:34 AM

DISA
A Combat Support Agency

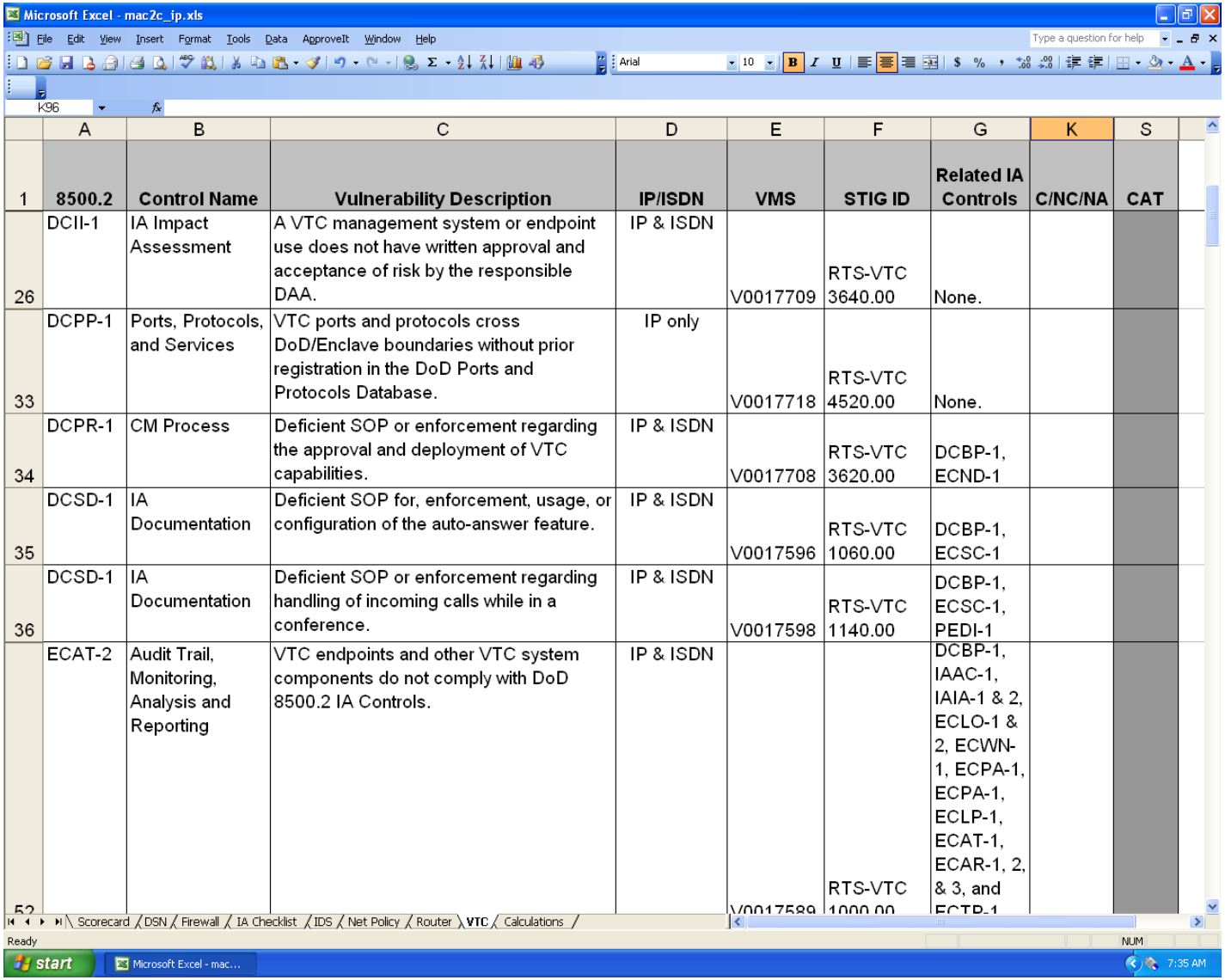
Step 1: Find the Correct Page

- You can see that there is a spreadsheet for each of the STIG tests.
- Click on the page that corresponds to the STIG test that you conducted.
- For example, you can see the Video Tele-conference (VTC) spreadsheet in the next slide.

DISA

A Combat Support Agency

Step 1: Find the Correct Page



	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
26	DCII-1	IA Impact Assessment	A VTC management system or endpoint use does not have written approval and acceptance of risk by the responsible DAA.	IP & ISDN	V0017709	RTS-VTC 3640.00	None.		
33	DCPP-1	Ports, Protocols, and Services	VTC ports and protocols cross DoD/Enclave boundaries without prior registration in the DoD Ports and Protocols Database.	IP only	V0017718	RTS-VTC 4520.00	None.		
34	DCPR-1	CM Process	Deficient SOP or enforcement regarding the approval and deployment of VTC capabilities.	IP & ISDN	V0017708	RTS-VTC 3620.00	DCBP-1, ECND-1		
35	DCSD-1	IA Documentation	Deficient SOP for, enforcement, usage, or configuration of the auto-answer feature.	IP & ISDN	V0017596	RTS-VTC 1060.00	DCBP-1, ECSC-1		
36	DCSD-1	IA Documentation	Deficient SOP or enforcement regarding handling of incoming calls while in a conference.	IP & ISDN	V0017598	RTS-VTC 1140.00	DCBP-1, ECSC-1, PEDI-1		
52	ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	VTC endpoints and other VTC system components do not comply with DoD 8500.2 IA Controls.	IP & ISDN	V0017589	RTS-VTC 1000.00	DCBP-1, IAAC-1, IAIA-1 & 2, ECLO-1 & 2, ECWN-1, ECPA-1, ECPA-1, ECLP-1, ECAT-1, ECAR-1, 2, & 3, and ECTP-1		

DISA
A Combat Support Agency

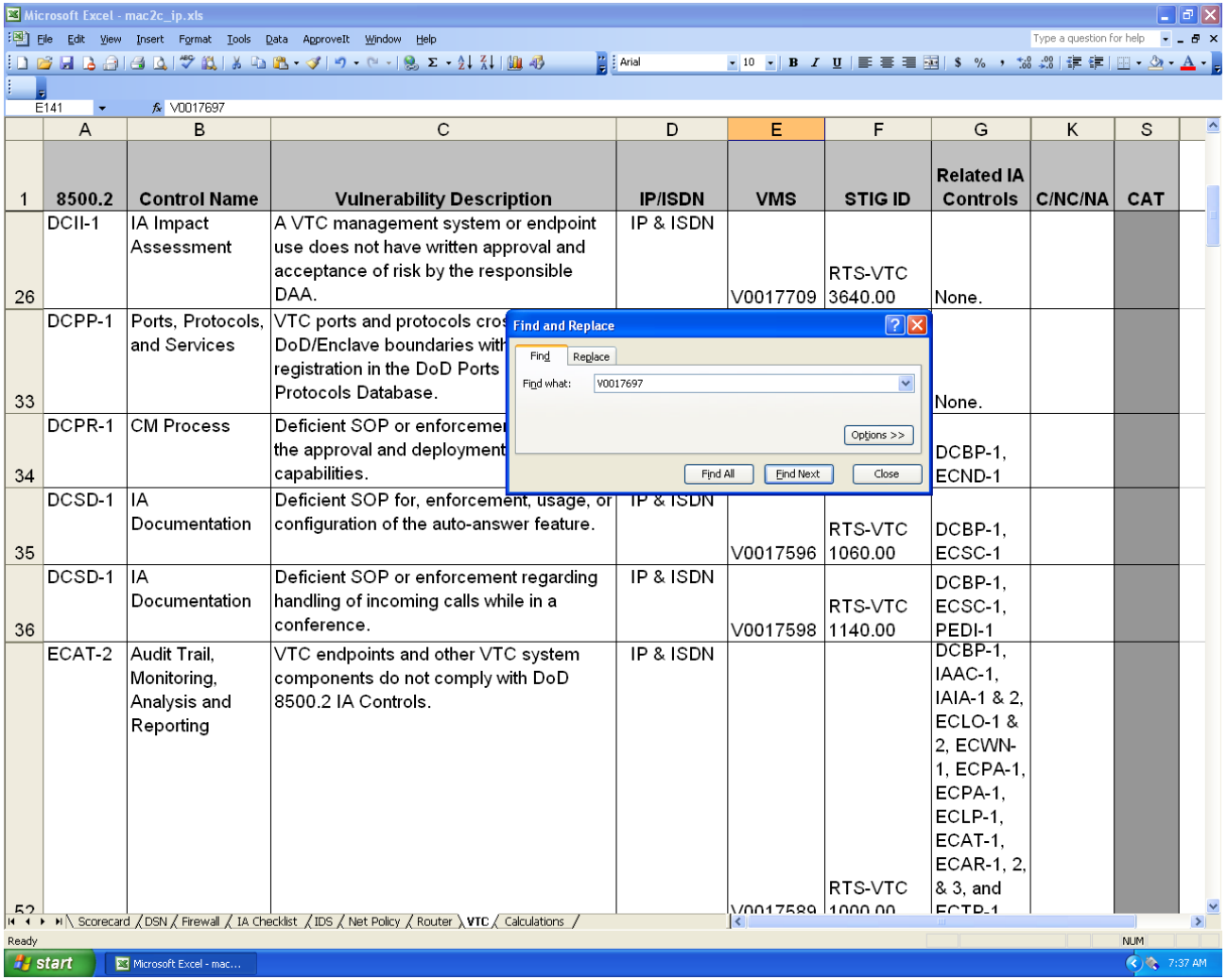
Step 2: Enter the Vulnerability

- Click “CTRL” and “F”.
- Enter a VMS vulnerability key.
- For instance, assuming V0017697 failed in your STIG test, enter V0017697.

DISA

A Combat Support Agency

Step 2: Enter the Vulnerability



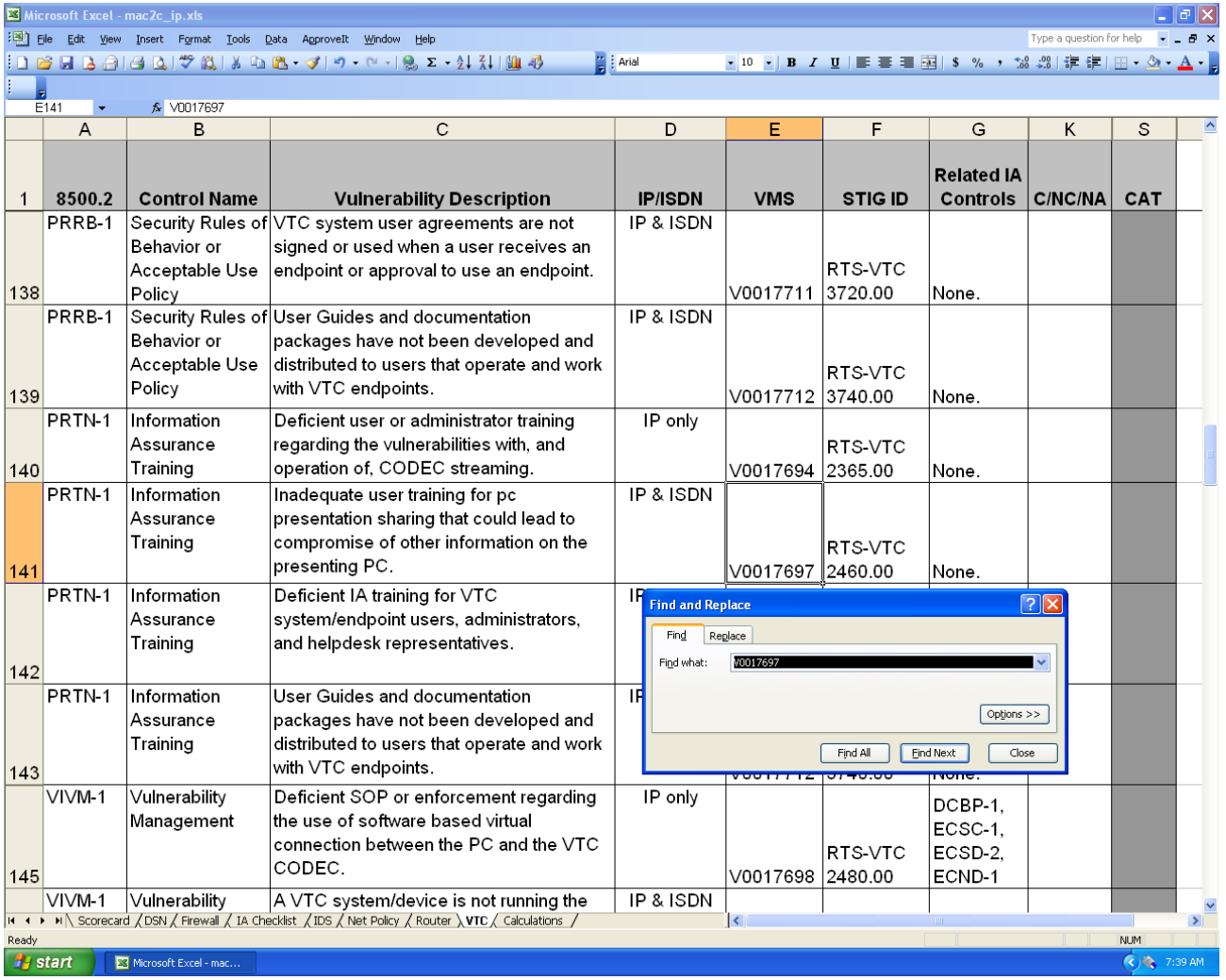
	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
26	DCII-1	IA Impact Assessment	A VTC management system or endpoint use does not have written approval and acceptance of risk by the responsible DAA.	IP & ISDN	V0017709	RTS-VTC 3640.00	None.		
33	DCPP-1	Ports, Protocols, and Services	VTC ports and protocols cros DoD/Enclave boundaries with registration in the DoD Ports Protocols Database.				None.		
34	DCPR-1	CM Process	Deficient SOP or enforcemer the approval and deployment capabilities.				DCBP-1, ECND-1		
35	DCSD-1	IA Documentation	Deficient SOP for, enforcement, usage, or configuration of the auto-answer feature.	IP & ISDN	V0017596	RTS-VTC 1060.00	DCBP-1, ECSC-1		
36	DCSD-1	IA Documentation	Deficient SOP or enforcement regarding handling of incoming calls while in a conference.	IP & ISDN	V0017598	RTS-VTC 1140.00	DCBP-1, ECSC-1, PEDI-1		
52	ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	VTC endpoints and other VTC system components do not comply with DoD 8500.2 IA Controls.	IP & ISDN	V0017589	RTS-VTC 1000.00	DCBP-1, IAAC-1, IAIA-1 & 2, ECLO-1 & 2, ECWN-1, ECPA-1, ECPA-1, ECLP-1, ECAT-1, ECAR-1, 2, & 3, and ECTP-1		

DISA

A Combat Support Agency

Step 2: Enter the Vulnerability

- **Then click the "Find Next" button.**
- **As you can see below, V0017697 is related to IA control PRTN-1.**

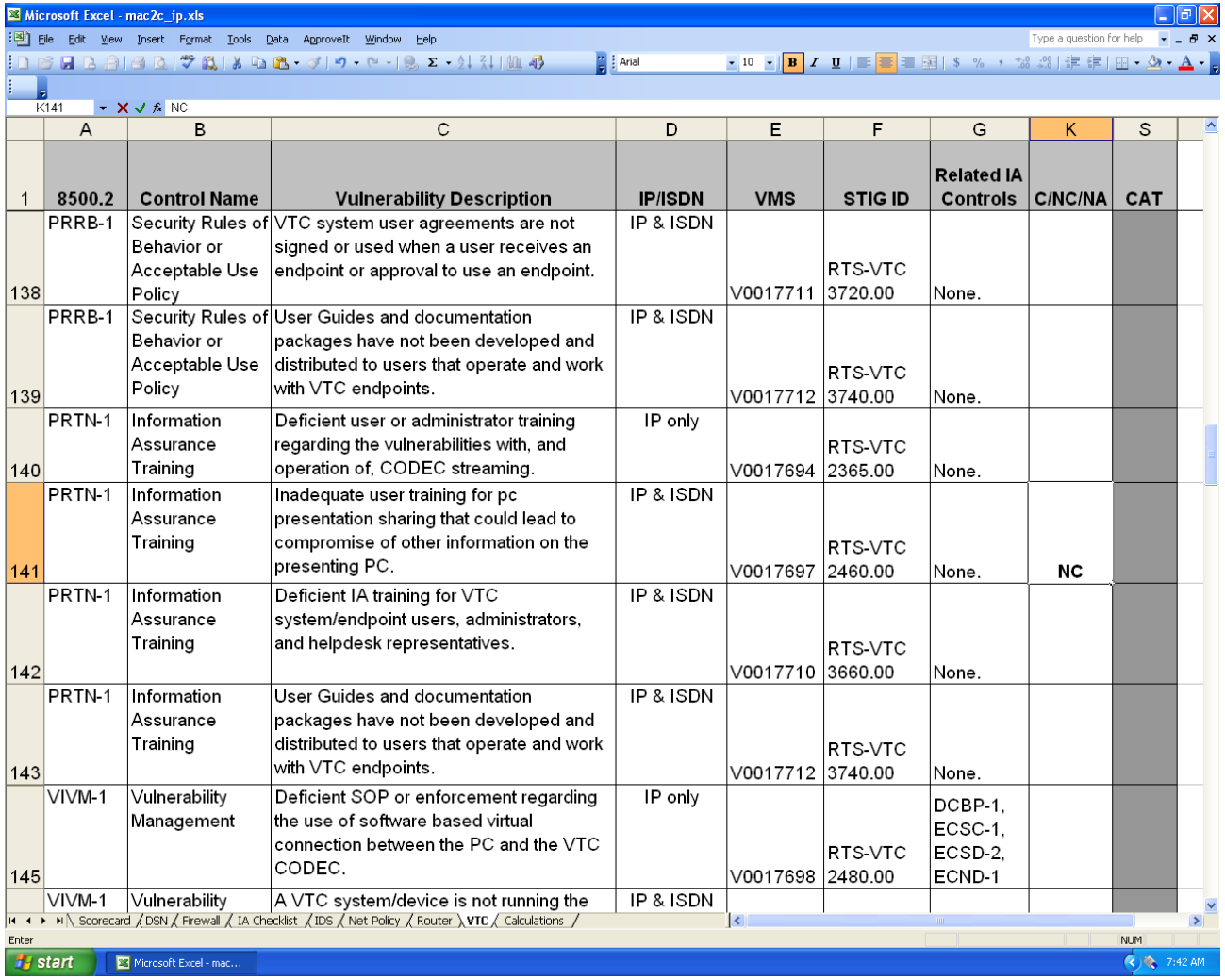


	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
138	PRRB-1	Security Rules of Behavior or Acceptable Use Policy	VTC system user agreements are not signed or used when a user receives an endpoint or approval to use an endpoint.	IP & ISDN	V0017711	RTS-VTC 3720.00	None.		
139	PRRB-1	Security Rules of Behavior or Acceptable Use Policy	User Guides and documentation packages have not been developed and distributed to users that operate and work with VTC endpoints.	IP & ISDN	V0017712	RTS-VTC 3740.00	None.		
140	PRTN-1	Information Assurance Training	Deficient user or administrator training regarding the vulnerabilities with, and operation of, CODEC streaming.	IP only	V0017694	RTS-VTC 2365.00	None.		
141	PRTN-1	Information Assurance Training	Inadequate user training for pc presentation sharing that could lead to compromise of other information on the presenting PC.	IP & ISDN	V0017697	RTS-VTC 2460.00	None.		
142	PRTN-1	Information Assurance Training	Deficient IA training for VTC system/endpoint users, administrators, and helpdesk representatives.	IP					
143	PRTN-1	Information Assurance Training	User Guides and documentation packages have not been developed and distributed to users that operate and work with VTC endpoints.	IP					
145	VIVM-1	Vulnerability Management	Deficient SOP or enforcement regarding the use of software based virtual connection between the PC and the VTC CODEC.	IP only	V0017698	RTS-VTC 2480.00	DCBP-1, ECSC-1, ECSD-2, ECND-1		
	VIVM-1	Vulnerability	A VTC system/device is not running the	IP & ISDN					

Step 3: Mark Compliance Status

A Combat Support Agency

- **In the C/NC/NA column of PRTN-1, enter "NC" for "Not Compliant" and then press "Enter."**

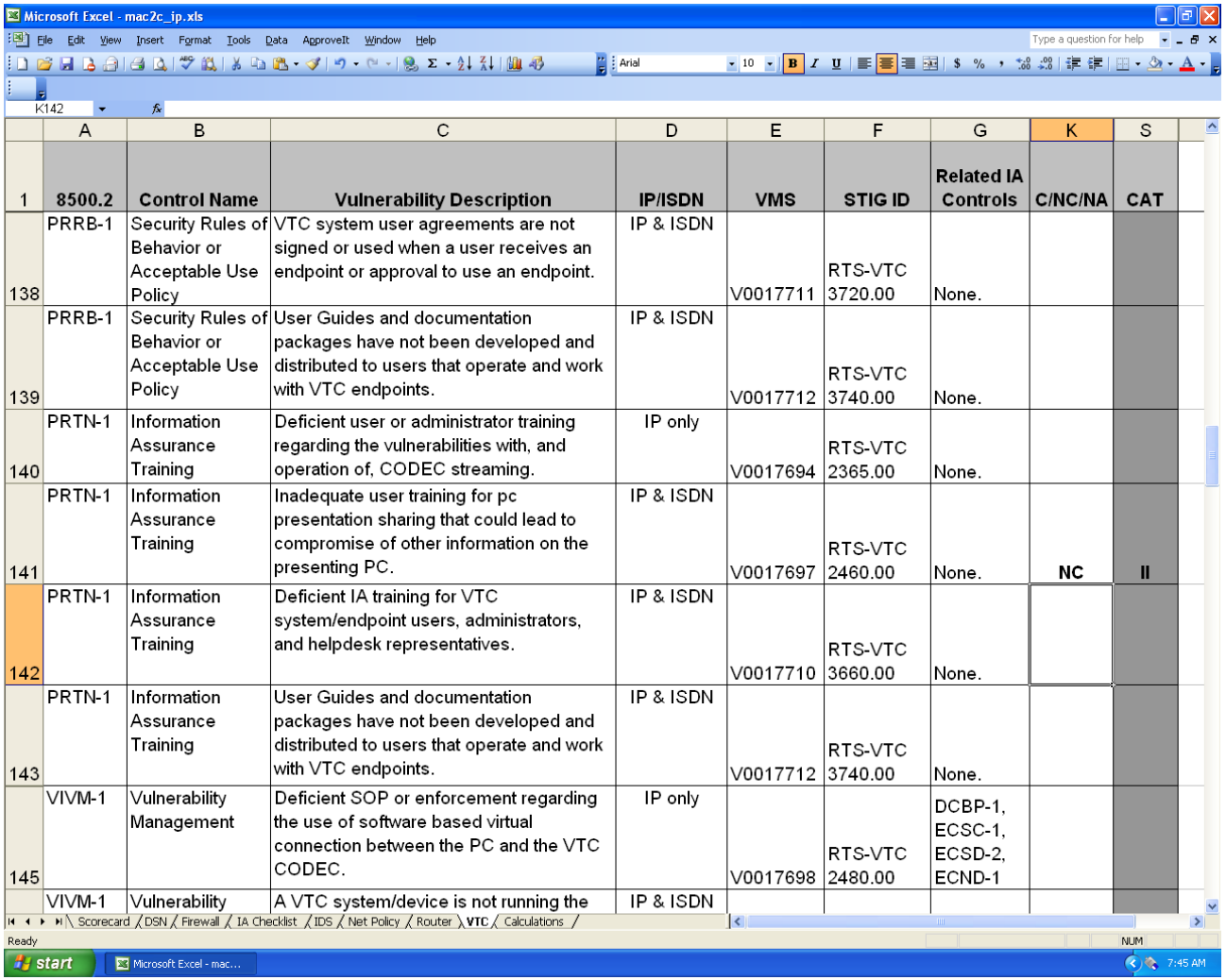


	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
138	PRRB-1	Security Rules of Behavior or Acceptable Use Policy	VTC system user agreements are not signed or used when a user receives an endpoint or approval to use an endpoint.	IP & ISDN	V0017711	RTS-VTC 3720.00	None.		
139	PRRB-1	Security Rules of Behavior or Acceptable Use Policy	User Guides and documentation packages have not been developed and distributed to users that operate and work with VTC endpoints.	IP & ISDN	V0017712	RTS-VTC 3740.00	None.		
140	PRTN-1	Information Assurance Training	Deficient user or administrator training regarding the vulnerabilities with, and operation of, CODEC streaming.	IP only	V0017694	RTS-VTC 2365.00	None.		
141	PRTN-1	Information Assurance Training	Inadequate user training for pc presentation sharing that could lead to compromise of other information on the presenting PC.	IP & ISDN	V0017697	RTS-VTC 2460.00	None.	NC	
142	PRTN-1	Information Assurance Training	Deficient IA training for VTC system/endpoint users, administrators, and helpdesk representatives.	IP & ISDN	V0017710	RTS-VTC 3660.00	None.		
143	PRTN-1	Information Assurance Training	User Guides and documentation packages have not been developed and distributed to users that operate and work with VTC endpoints.	IP & ISDN	V0017712	RTS-VTC 3740.00	None.		
145	VIVM-1	Vulnerability Management	Deficient SOP or enforcement regarding the use of software based virtual connection between the PC and the VTC CODEC.	IP only	V0017698	RTS-VTC 2480.00	DCBP-1, ECSC-1, ECSD-2, ECND-1		
	VIVM-1	Vulnerability	A VTC system/device is not running the	IP & ISDN					

Step 3: Mark Compliance Status

A Combat Support Agency

- **As you can see below, the severity category for PRTN-1 (CAT II) appears automatically.**

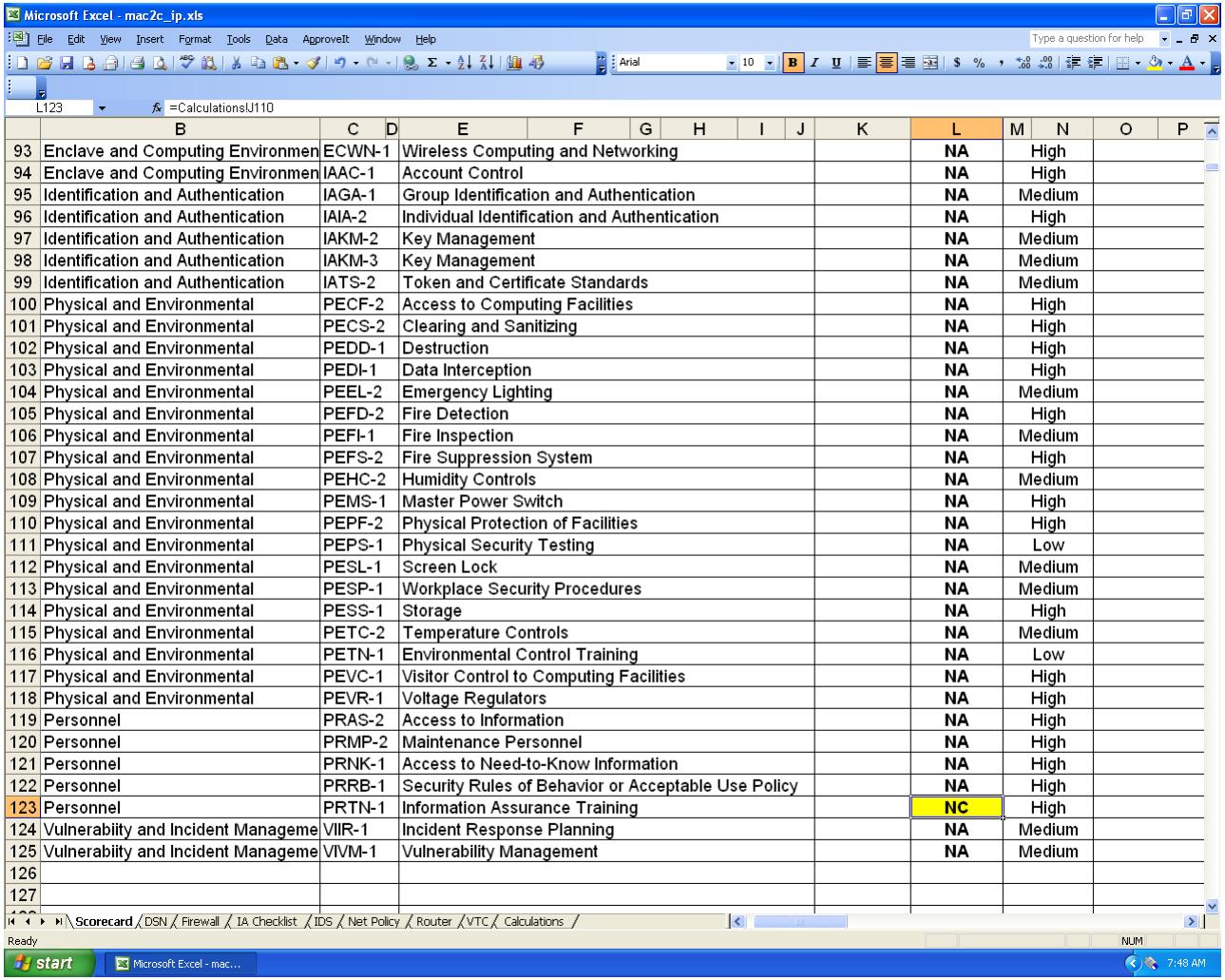


	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
138	PRRB-1	Security Rules of Behavior or Acceptable Use Policy	VTC system user agreements are not signed or used when a user receives an endpoint or approval to use an endpoint.	IP & ISDN	V0017711	RTS-VTC 3720.00	None.		
139	PRRB-1	Security Rules of Behavior or Acceptable Use Policy	User Guides and documentation packages have not been developed and distributed to users that operate and work with VTC endpoints.	IP & ISDN	V0017712	RTS-VTC 3740.00	None.		
140	PRTN-1	Information Assurance Training	Deficient user or administrator training regarding the vulnerabilities with, and operation of, CODEC streaming.	IP only	V0017694	RTS-VTC 2365.00	None.		
141	PRTN-1	Information Assurance Training	Inadequate user training for pc presentation sharing that could lead to compromise of other information on the presenting PC.	IP & ISDN	V0017697	RTS-VTC 2460.00	None.	NC	II
142	PRTN-1	Information Assurance Training	Deficient IA training for VTC system/endpoint users, administrators, and helpdesk representatives.	IP & ISDN	V0017710	RTS-VTC 3660.00	None.		
143	PRTN-1	Information Assurance Training	User Guides and documentation packages have not been developed and distributed to users that operate and work with VTC endpoints.	IP & ISDN	V0017712	RTS-VTC 3740.00	None.		
145	VIVM-1	Vulnerability Management	Deficient SOP or enforcement regarding the use of software based virtual connection between the PC and the VTC CODEC.	IP only	V0017698	RTS-VTC 2480.00	DCBP-1, ECSC-1, ECSD-2, ECND-1		
	VIVM-1	Vulnerability	A VTC system/device is not running the	IP & ISDN					

Step 3: Mark Compliance Status

A Combat Support Agency

- **Now go to the Scorecard page. You can see that PRTN-1 is “NC”.**

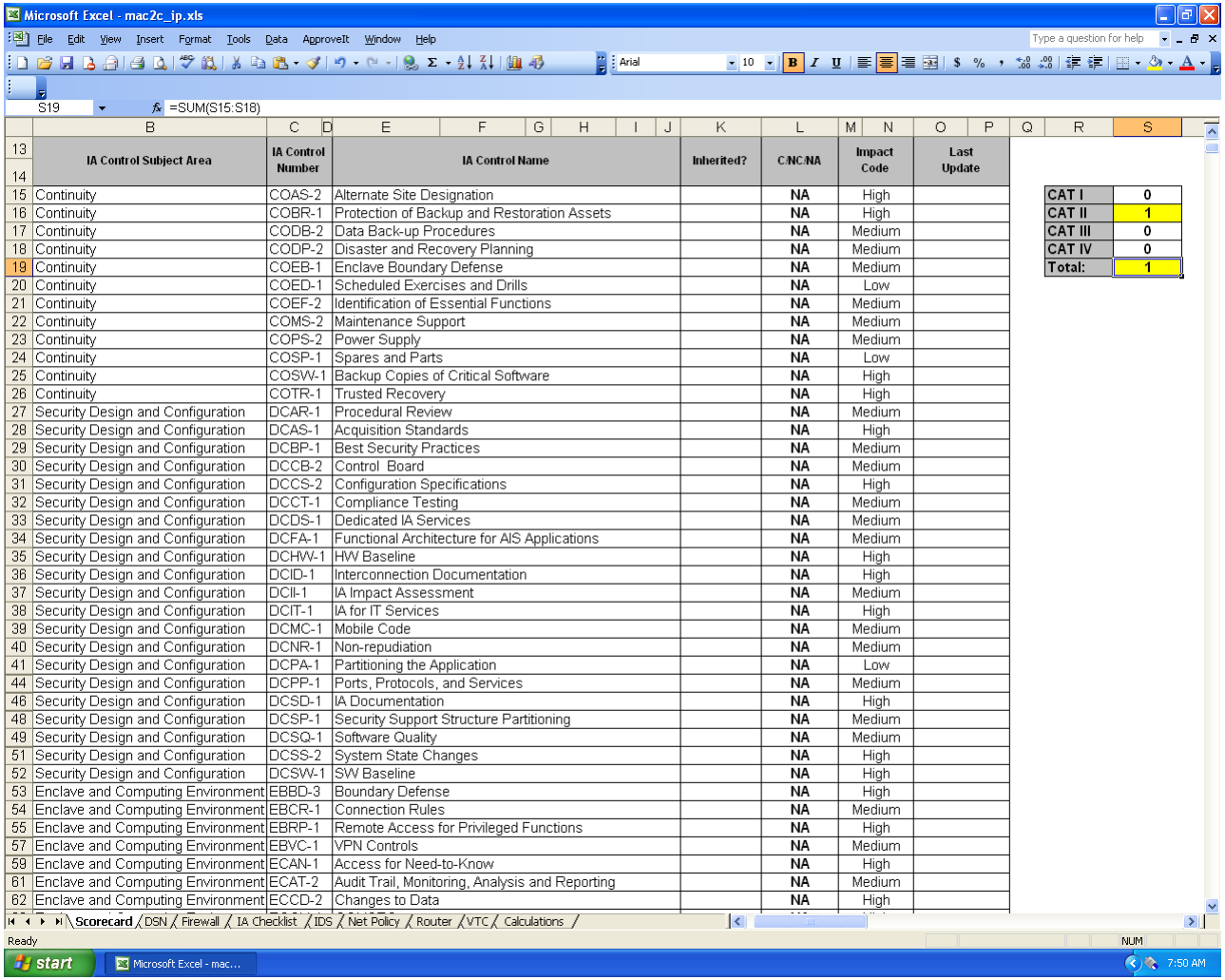


	B	C	E	L	N
93	Enclave and Computing Environmen	ECWN-1	Wireless Computing and Networking	NA	High
94	Enclave and Computing Environmen	IAAC-1	Account Control	NA	High
95	Identification and Authentication	IAGA-1	Group Identification and Authentication	NA	Medium
96	Identification and Authentication	IAIA-2	Individual Identification and Authentication	NA	High
97	Identification and Authentication	IAKM-2	Key Management	NA	Medium
98	Identification and Authentication	IAKM-3	Key Management	NA	Medium
99	Identification and Authentication	IATS-2	Token and Certificate Standards	NA	Medium
100	Physical and Environmental	PECF-2	Access to Computing Facilities	NA	High
101	Physical and Environmental	PECS-2	Clearing and Sanitizing	NA	High
102	Physical and Environmental	PEDD-1	Destruction	NA	High
103	Physical and Environmental	PEDI-1	Data Interception	NA	High
104	Physical and Environmental	PEEL-2	Emergency Lighting	NA	Medium
105	Physical and Environmental	PEFD-2	Fire Detection	NA	High
106	Physical and Environmental	PEFI-1	Fire Inspection	NA	Medium
107	Physical and Environmental	PEFS-2	Fire Suppression System	NA	High
108	Physical and Environmental	PEHC-2	Humidity Controls	NA	Medium
109	Physical and Environmental	PEMS-1	Master Power Switch	NA	High
110	Physical and Environmental	PEPF-2	Physical Protection of Facilities	NA	High
111	Physical and Environmental	PEPS-1	Physical Security Testing	NA	Low
112	Physical and Environmental	PESL-1	Screen Lock	NA	Medium
113	Physical and Environmental	PESP-1	Workplace Security Procedures	NA	Medium
114	Physical and Environmental	PESS-1	Storage	NA	High
115	Physical and Environmental	PETC-2	Temperature Controls	NA	Medium
116	Physical and Environmental	PETN-1	Environmental Control Training	NA	Low
117	Physical and Environmental	PEVC-1	Visitor Control to Computing Facilities	NA	High
118	Physical and Environmental	PEVR-1	Voltage Regulators	NA	High
119	Personnel	PRAS-2	Access to Information	NA	High
120	Personnel	PRMP-2	Maintenance Personnel	NA	High
121	Personnel	PRNK-1	Access to Need-to-Know Information	NA	High
122	Personnel	PRRB-1	Security Rules of Behavior or Acceptable Use Policy	NA	High
123	Personnel	PRTN-1	Information Assurance Training	NC	High
124	Vulnerabiity and Incident Manageme	VIIR-1	Incident Response Planning	NA	Medium
125	Vulnerabiity and Incident Manageme	VIVM-1	Vulnerability Management	NA	Medium
126					
127					

Step 3: Mark Compliance Status

A Combat Support Agency

- **You can also see that there is now one CAT II vulnerability in the severity category table on the Scorecard page.**



Microsoft Excel - mac2c_ip.xls

File Edit View Insert Format Tools Data AproveIt Window Help

S19 =SUM(S15:S18)

IA Control Subject Area	IA Control Number	IA Control Name	Inherited?	C/NC/NA	Impact Code	Last Update
Continuity	COAS-2	Alternate Site Designation		NA	High	
Continuity	COBR-1	Protection of Backup and Restoration Assets		NA	High	
Continuity	CODB-2	Data Back-up Procedures		NA	Medium	
Continuity	CODP-2	Disaster and Recovery Planning		NA	Medium	
Continuity	COEB-1	Enclave Boundary Defense		NA	Medium	
Continuity	COED-1	Scheduled Exercises and Drills		NA	Low	
Continuity	COEF-2	Identification of Essential Functions		NA	Medium	
Continuity	COMS-2	Maintenance Support		NA	Medium	
Continuity	COPS-2	Power Supply		NA	Medium	
Continuity	COSP-1	Spares and Parts		NA	Low	
Continuity	COSW-1	Backup Copies of Critical Software		NA	High	
Continuity	COTR-1	Trusted Recovery		NA	High	
Security Design and Configuration	DCAR-1	Procedural Review		NA	Medium	
Security Design and Configuration	DCAS-1	Acquisition Standards		NA	High	
Security Design and Configuration	DCBP-1	Best Security Practices		NA	Medium	
Security Design and Configuration	DCCB-2	Control Board		NA	Medium	
Security Design and Configuration	DCCS-2	Configuration Specifications		NA	High	
Security Design and Configuration	DCCT-1	Compliance Testing		NA	Medium	
Security Design and Configuration	DCDS-1	Dedicated IA Services		NA	Medium	
Security Design and Configuration	DCFA-1	Functional Architecture for AIS Applications		NA	Medium	
Security Design and Configuration	DCHW-1	HW Baseline		NA	High	
Security Design and Configuration	DCID-1	Interconnection Documentation		NA	High	
Security Design and Configuration	DCII-1	IA Impact Assessment		NA	Medium	
Security Design and Configuration	DCIT-1	IA for IT Services		NA	High	
Security Design and Configuration	DCMC-1	Mobile Code		NA	Medium	
Security Design and Configuration	DCNR-1	Non-repudiation		NA	Medium	
Security Design and Configuration	DCPA-1	Partitioning the Application		NA	Low	
Security Design and Configuration	DCPP-1	Ports, Protocols, and Services		NA	Medium	
Security Design and Configuration	DCSD-1	IA Documentation		NA	High	
Security Design and Configuration	DCSP-1	Security Support Structure Partitioning		NA	Medium	
Security Design and Configuration	DCSQ-1	Software Quality		NA	Medium	
Security Design and Configuration	DCSS-2	System State Changes		NA	High	
Security Design and Configuration	DCSW-1	SW Baseline		NA	High	
Enclave and Computing Environment	EBBD-3	Boundary Defense		NA	High	
Enclave and Computing Environment	EBCR-1	Connection Rules		NA	Medium	
Enclave and Computing Environment	EBRP-1	Remote Access for Privileged Functions		NA	High	
Enclave and Computing Environment	EBVC-1	VPN Controls		NA	Medium	
Enclave and Computing Environment	ECAN-1	Access for Need-to-Know		NA	High	
Enclave and Computing Environment	ECAT-2	Audit Trail, Monitoring, Analysis and Reporting		NA	Medium	
Enclave and Computing Environment	ECCD-2	Changes to Data		NA	High	

CAT I	0
CAT II	1
CAT III	0
CAT IV	0
Total:	1

Scorecard / DSN / Firewall / IA Checklist / IDS / Net Policy / Router / VTC / Calculations /

Ready NUM

start Microsoft Excel - mac... 7:50 AM

DISA
A Combat Support Agency

More Instructions

- You should repeat these steps for all STIG test results until you have a completed Scorecard.
- Remember, since all IA controls on the Scorecard default to “NA” (Not Applicable), in the IA Checklist page, every IA control must be appropriately marked “C”, “NC”, or “NA.”
- Otherwise, the Scorecard might show that the IA control is “NA” when it really is not.
- More guidance on how to complete the Scorecard Matrix is in the slides that follow.

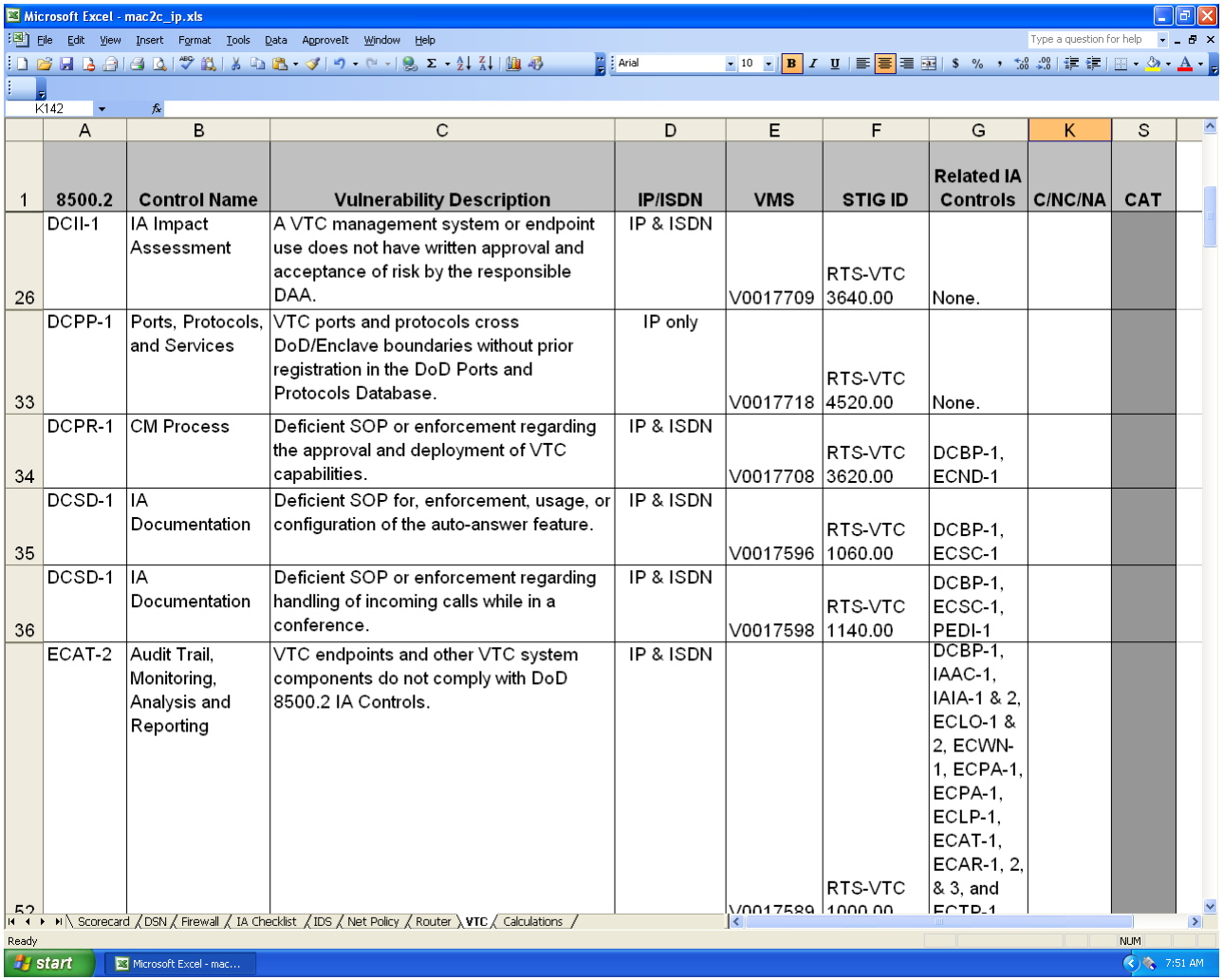
DISA
A Combat Support Agency

Severity Categories

- **Remember that many vulnerabilities in the STIGs are linked to more than one IA control.**
- **If one vulnerability fails, then all related IA controls will fail.**
- **However, only one severity category will be recorded for each vulnerability.**
- **For example, if one CAT I vulnerability fails three IA controls, you still have only one CAT I.**
- **Thus, in many cases, not every failed IA control will be assigned a severity category.**
- **However, all vulnerabilities are assigned a severity category in accordance with the STIGs.**

Back to VTC Page

- **Let's practice more. Go back to the VTC page.**



Microsoft Excel - mac2c_ip.xls

K142

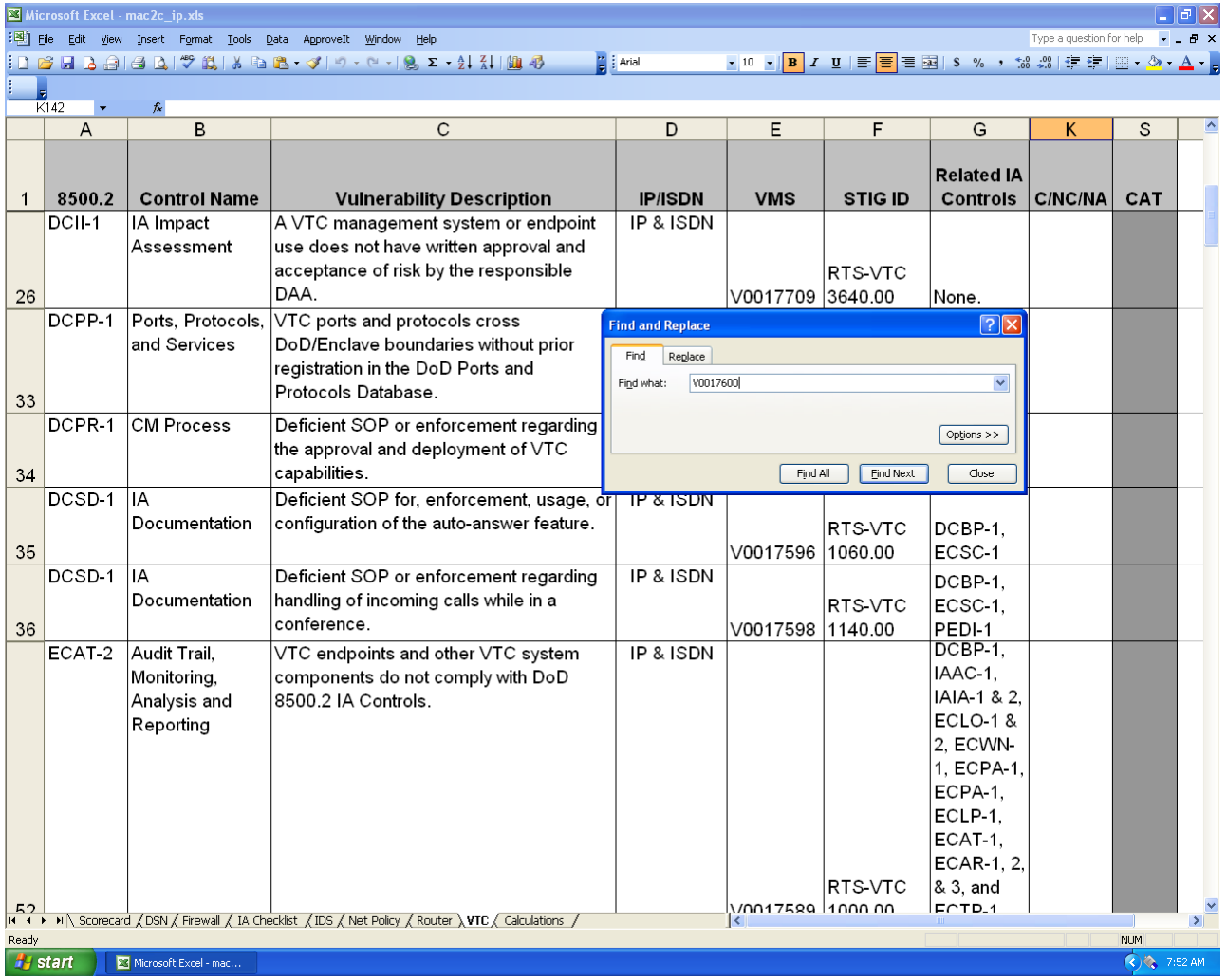
	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
26	DCII-1	IA Impact Assessment	A VTC management system or endpoint use does not have written approval and acceptance of risk by the responsible DAA.	IP & ISDN	V0017709	RTS-VTC 3640.00	None.		
33	DCPP-1	Ports, Protocols, and Services	VTC ports and protocols cross DoD/Enclave boundaries without prior registration in the DoD Ports and Protocols Database.	IP only	V0017718	RTS-VTC 4520.00	None.		
34	DCPR-1	CM Process	Deficient SOP or enforcement regarding the approval and deployment of VTC capabilities.	IP & ISDN	V0017708	RTS-VTC 3620.00	DCBP-1, ECND-1		
35	DCSD-1	IA Documentation	Deficient SOP for, enforcement, usage, or configuration of the auto-answer feature.	IP & ISDN	V0017596	RTS-VTC 1060.00	DCBP-1, ECSC-1		
36	DCSD-1	IA Documentation	Deficient SOP or enforcement regarding handling of incoming calls while in a conference.	IP & ISDN	V0017598	RTS-VTC 1140.00	DCBP-1, ECSC-1, PEDI-1		
52	ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	VTC endpoints and other VTC system components do not comply with DoD 8500.2 IA Controls.	IP & ISDN	V0017589	RTS-VTC 1000.00	DCBP-1, IAAC-1, IAIA-1 & 2, ECLO-1 & 2, ECWN-1, ECPA-1, ECPA-1, ECLP-1, ECAT-1, ECAR-1, 2, & 3, and ECTP-1		

Scorecard | DSN | Firewall | IA Checklist | IDS | Net Policy | Router | VTC | Calculations

Ready

Enter V0017600

- **Press “CTRL” and “F” and enter V0017600.**

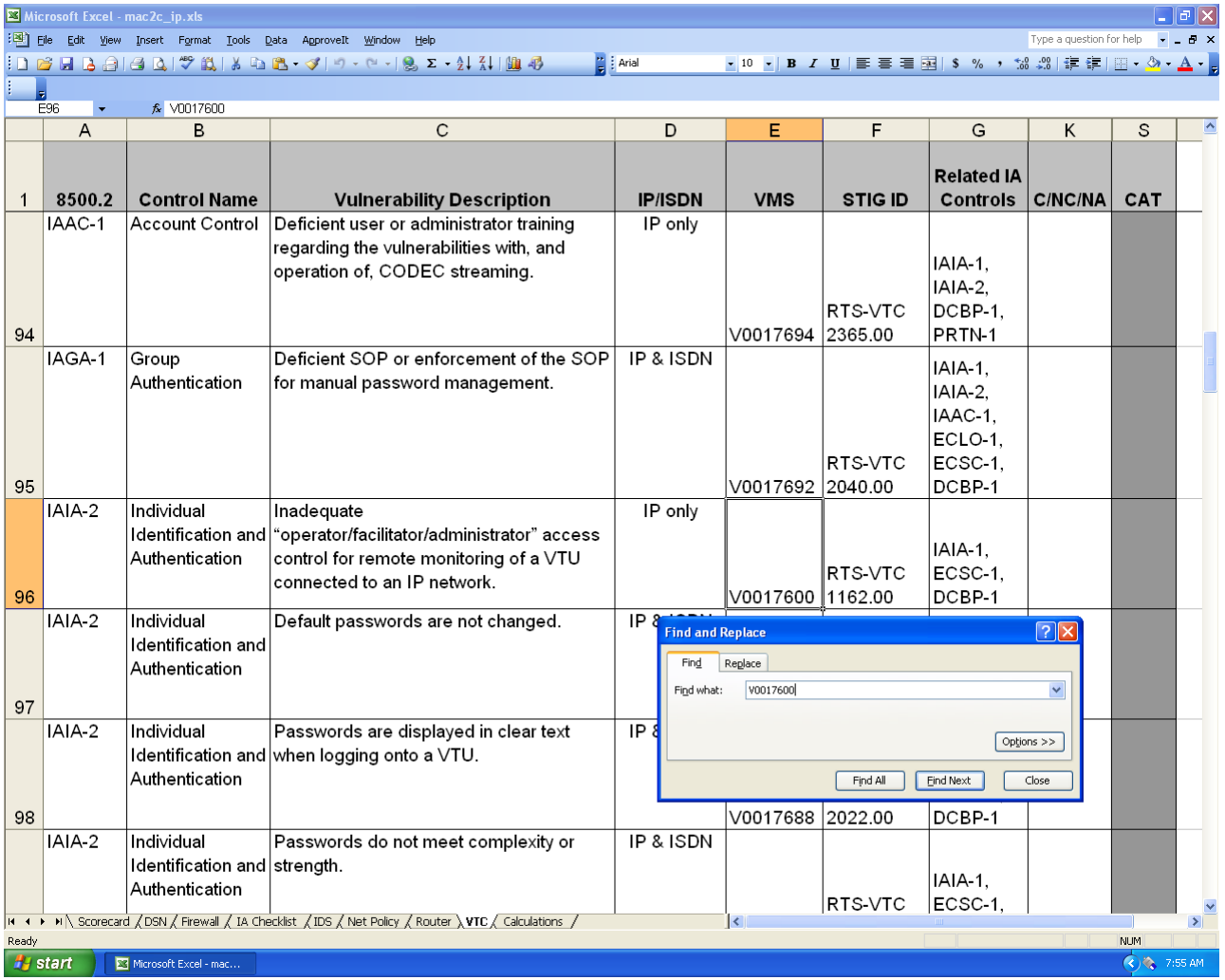


	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
26	DCII-1	IA Impact Assessment	A VTC management system or endpoint use does not have written approval and acceptance of risk by the responsible DAA.	IP & ISDN	V0017709	RTS-VTC 3640.00	None.		
33	DCPP-1	Ports, Protocols, and Services	VTC ports and protocols cross DoD/Enclave boundaries without prior registration in the DoD Ports and Protocols Database.						
34	DCPR-1	CM Process	Deficient SOP or enforcement regarding the approval and deployment of VTC capabilities.						
35	DCSD-1	IA Documentation	Deficient SOP for, enforcement, usage, or configuration of the auto-answer feature.	IP & ISDN	V0017596	RTS-VTC 1060.00	DCBP-1, ECSC-1		
36	DCSD-1	IA Documentation	Deficient SOP or enforcement regarding handling of incoming calls while in a conference.	IP & ISDN	V0017598	RTS-VTC 1140.00	DCBP-1, ECSC-1, PEDI-1		
52	ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	VTC endpoints and other VTC system components do not comply with DoD 8500.2 IA Controls.	IP & ISDN	V0017589	RTS-VTC 1000.00	DCBP-1, IAAC-1, IAIA-1 & 2, ECLO-1 & 2, ECWN-1, ECPA-1, ECPA-1, ECLP-1, ECAT-1, ECAR-1, 2, & 3, and ECTP-1		

V0017600 & IAIA-2

A Combat Support Agency

- **Click "Find Next." Notice below that vulnerability V0017600 is tied to IA control IAIA-2.**



	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
94	IAAC-1	Account Control	Deficient user or administrator training regarding the vulnerabilities with, and operation of, CODEC streaming.	IP only	V0017694	RTS-VTC 2365.00	IAIA-1, IAIA-2, DCBP-1, PRTN-1		
95	IAGA-1	Group Authentication	Deficient SOP or enforcement of the SOP for manual password management.	IP & ISDN	V0017692	RTS-VTC 2040.00	IAIA-1, IAIA-2, IAAC-1, ECLO-1, ECSC-1, DCBP-1		
96	IAIA-2	Individual Identification and Authentication	Inadequate "operator/facilitator/administrator" access control for remote monitoring of a VTU connected to an IP network.	IP only	V0017600	RTS-VTC 1162.00	IAIA-1, ECSC-1, DCBP-1		
97	IAIA-2	Individual Identification and Authentication	Default passwords are not changed.	IP &					
98	IAIA-2	Individual Identification and Authentication	Passwords are displayed in clear text when logging onto a VTU.	IP &	V0017688	2022.00	DCBP-1		
	IAIA-2	Individual Identification and Authentication	Passwords do not meet complexity or strength.	IP & ISDN		RTS-VTC	IAIA-1, ECSC-1,		

Related IA Controls

A Combat Support Agency

- **Also notice that ECSC-1, DCBP-1 are listed in the Related IA Controls column of the IAIA-2 row.**

Microsoft Excel - mac2c_ip.xls

File Edit View Insert Format Tools Data ApproveIt Window Help

G96 ECSC-1, DCBP-1

	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
94	IAAC-1	Account Control	Deficient user or administrator training regarding the vulnerabilities with, and operation of, CODEC streaming.	IP only	V0017694	RTS-VTC 2365.00	IAIA-1, IAIA-2, DCBP-1, PRTN-1		
95	IAGA-1	Group Authentication	Deficient SOP or enforcement of the SOP for manual password management.	IP & ISDN	V0017692	RTS-VTC 2040.00	IAIA-1, IAIA-2, IAAC-1, ECLO-1, ECSC-1, DCBP-1		
96	IAIA-2	Individual Identification and Authentication	Inadequate "operator/facilitator/administrator" access control for remote monitoring of a VTU connected to an IP network.	IP only	V0017600	RTS-VTC 1162.00	ECSC-1, DCBP-1		
97	IAIA-2	Individual Identification and Authentication	Default passwords are not changed.	IP & ISDN	V0017687	RTS-VTC 2020.00	IAIA-1, ECSC-1, DCBP-1		
98	IAIA-2	Individual Identification and Authentication	Passwords are displayed in clear text when logging onto a VTU.	IP & ISDN	V0017688	RTS-VTC 2022.00	IAIA-1, ECSC-1, DCBP-1		
	IAIA-2	Individual Identification and Authentication	Passwords do not meet complexity or strength.	IP & ISDN		RTS-VTC	IAIA-1, ECSC-1,		

Scorecard / DSN / Firewall / IA Checklist / IDS / Net Policy / Router / VTC / Calculations /

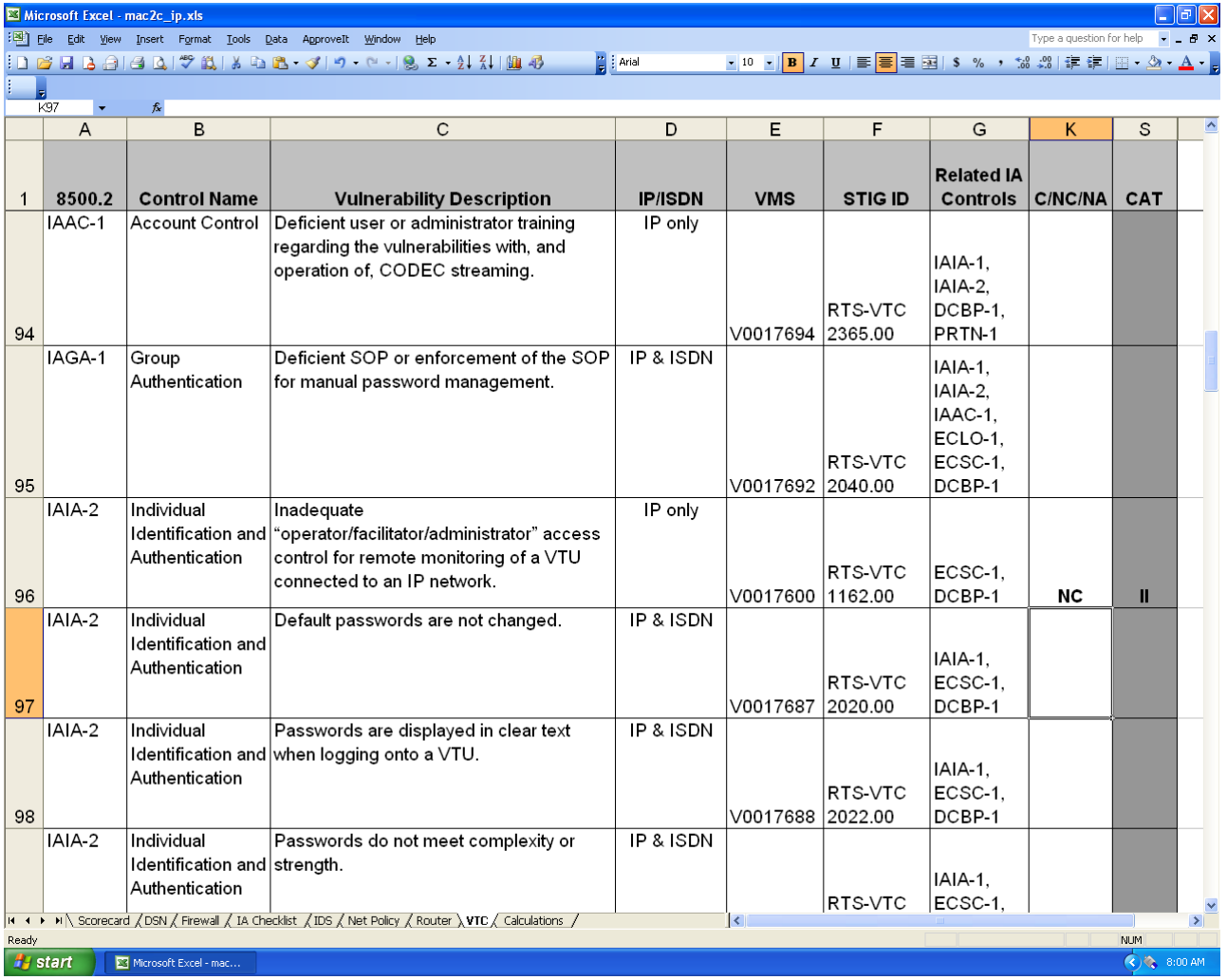
Edit NUM

start Microsoft Excel - mac... 7:57 AM

A Combat Support Agency

IAIA-2 Is CAT II

- **Enter "NC" and press enter. As you can see below, the severity category for this vulnerability is CAT II.**



	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
94	IAAC-1	Account Control	Deficient user or administrator training regarding the vulnerabilities with, and operation of, CODEC streaming.	IP only	V0017694	RTS-VTC 2365.00	IAIA-1, IAIA-2, DCBP-1, PRTN-1		
95	IAGA-1	Group Authentication	Deficient SOP or enforcement of the SOP for manual password management.	IP & ISDN	V0017692	RTS-VTC 2040.00	IAIA-1, IAIA-2, IAAC-1, ECLO-1, ECSC-1, DCBP-1		
96	IAIA-2	Individual Identification and Authentication	Inadequate "operator/facilitator/administrator" access control for remote monitoring of a VTU connected to an IP network.	IP only	V0017600	RTS-VTC 1162.00	ECSC-1, DCBP-1	NC	II
97	IAIA-2	Individual Identification and Authentication	Default passwords are not changed.	IP & ISDN	V0017687	RTS-VTC 2020.00	IAIA-1, ECSC-1, DCBP-1		
98	IAIA-2	Individual Identification and Authentication	Passwords are displayed in clear text when logging onto a VTU.	IP & ISDN	V0017688	RTS-VTC 2022.00	IAIA-1, ECSC-1, DCBP-1		
	IAIA-2	Individual Identification and Authentication	Passwords do not meet complexity or strength.	IP & ISDN		RTS-VTC	IAIA-1, ECSC-1,		

IAIA-2 “NC” on Scorecard

A Combat Support Agency

- **Now look at the Scorecard. Notice that IAIA-2 Fails.**

Microsoft Excel - mac2c_ip.xls

File Edit View Insert Format Tools Data ApproveIt Window Help

L96 =CalculationsIJ83

	B	C	E	L	M	N
85	Enclave and Computing Environmen	ECSD-2	Software Development Change Controls	NA	High	
86	Enclave and Computing Environmen	ECTB-1	Audit Trail Backup	NA	Medium	
87	Enclave and Computing Environmen	ECTC-1	Tempest Controls	NA	High	
88	Enclave and Computing Environmen	ECTM-2	Transmission Integrity Controls	NA	Medium	
89	Enclave and Computing Environmen	ECTP-1	Audit Trail Protection	NA	Medium	
90	Enclave and Computing Environmen	ECVI-1	Voice over IP	NA	Medium	
91	Enclave and Computing Environmen	ECVP-1	Virus Protection	NA	High	
92	Enclave and Computing Environmen	ECWM-1	Warning Message	NA	Low	
93	Enclave and Computing Environmen	ECWN-1	Wireless Computing and Networking	NA	High	
94	Enclave and Computing Environmen	IAAC-1	Account Control	NA	High	
95	Identification and Authentication	IAGA-1	Group Identification and Authentication	NA	Medium	
96	Identification and Authentication	IAIA-2	Individual Identification and Authentication	NC	High	
97	Identification and Authentication	IAKM-2	Key Management	NA	Medium	
98	Identification and Authentication	IAKM-3	Key Management	NA	Medium	
99	Identification and Authentication	IATS-2	Token and Certificate Standards	NA	Medium	
100	Physical and Environmental	PECF-2	Access to Computing Facilities	NA	High	
101	Physical and Environmental	PECS-2	Clearing and Sanitizing	NA	High	
102	Physical and Environmental	PEDD-1	Destruction	NA	High	
103	Physical and Environmental	PEDI-1	Data Interception	NA	High	
104	Physical and Environmental	PEEL-2	Emergency Lighting	NA	Medium	
105	Physical and Environmental	PEFD-2	Fire Detection	NA	High	
106	Physical and Environmental	PEFI-1	Fire Inspection	NA	Medium	
107	Physical and Environmental	PEFS-2	Fire Suppression System	NA	High	
108	Physical and Environmental	PEHC-2	Humidity Controls	NA	Medium	
109	Physical and Environmental	PEMS-1	Master Power Switch	NA	High	
110	Physical and Environmental	PEPF-2	Physical Protection of Facilities	NA	High	
111	Physical and Environmental	PEPS-1	Physical Security Testing	NA	Low	
112	Physical and Environmental	PESL-1	Screen Lock	NA	Medium	
113	Physical and Environmental	PESP-1	Workplace Security Procedures	NA	Medium	
114	Physical and Environmental	PESS-1	Storage	NA	High	
115	Physical and Environmental	PETC-2	Temperature Controls	NA	Medium	
116	Physical and Environmental	PETN-1	Environmental Control Training	NA	Low	
117	Physical and Environmental	PEVC-1	Visitor Control to Computing Facilities	NA	High	
118	Physical and Environmental	PEVR-1	Voltage Regulators	NA	High	
119	Personnel	PRAS-2	Access to Information	NA	High	

Scorecard / DSN / Firewall / IA Checklist / IDS / Net Policy / Router / VTC / Calculations /

Ready NUM

start Microsoft Excel - mac... 8:01 AM

ECSC-1 & DCBP-1 Also “NC”

A Combat Support Agency

- **Also notice that ECSC-1 and DCBP-1 fail on the Scorecard, too.**

Microsoft Excel - mac2c_ip.xls

=CalculationsU16

	B	C	E	L	N
29	Security Design and Configuration	DCBP-1	Best Security Practices	NC	Medium
30	Security Design and Configuration	DCCB-2	Control Board	NA	Medium
31	Security Design and Configuration	DCCS-2	Configuration Specifications	NA	High
32	Security Design and Configuration	DCCT-1	Compliance Testing	NA	Medium
33	Security Design and Configuration	DCDS-1	Dedicated IA Services	NA	Medium
34	Security Design and Configuration	DCFA-1	Functional Architecture for AIS Applications	NA	Medium
35	Security Design and Configuration	DCHW-1	HW Baseline	NA	High
36	Security Design and Configuration	DCID-1	Interconnection Documentation	NA	High
37	Security Design and Configuration	DCII-1	IA Impact Assessment	NA	Medium
38	Security Design and Configuration	DCIT-1	IA for IT Services	NA	High
39	Security Design and Configuration	DCMC-1	Mobile Code	NA	Medium
40	Security Design and Configuration	DCNR-1	Non-repudiation	NA	Medium
41	Security Design and Configuration	DCPA-1	Partitioning the Application	NA	Low
44	Security Design and Configuration	DCPP-1	Ports, Protocols, and Services	NA	Medium
46	Security Design and Configuration	DCSD-1	IA Documentation	NA	High
48	Security Design and Configuration	DCSP-1	Security Support Structure Partitioning	NA	Medium
49	Security Design and Configuration	DCSQ-1	Software Quality	NA	Medium
51	Security Design and Configuration	DCSS-2	System State Changes	NA	High
52	Security Design and Configuration	DCSW-1	SW Baseline	NA	High
53	Enclave and Computing Environment	EBBD-3	Boundary Defense	NA	High
54	Enclave and Computing Environment	EBCR-1	Connection Rules	NA	Medium
55	Enclave and Computing Environment	EBRP-1	Remote Access for Privileged Functions	NA	High
57	Enclave and Computing Environment	EBVC-1	VPN Controls	NA	Medium
59	Enclave and Computing Environment	ECAN-1	Access for Need-to-Know	NA	High
61	Enclave and Computing Environment	ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	NA	Medium
62	Enclave and Computing Environment	ECCD-2	Changes to Data	NA	High
63	Enclave and Computing Environment	ECCM-1	COMSEC	NA	High
65	Enclave and Computing Environment	ECCR-3	Encryption for Confidentiality (Data at Rest)	NA	High
66	Enclave and Computing Environment	ECCT-2	Encryption for Confidentiality (Data in Transit)	NA	High
67	Enclave and Computing Environment	ECDC-1	Data Change Controls	NA	Medium
68	Enclave and Computing Environment	ECIC-1	Interconnection among DoD Systems and Enclaves	NA	Medium
69	Enclave and Computing Environment	ECID-1	Host Based IDS	NA	Medium
71	Enclave and Computing Environment	ECLC-1	Audit of Security Label Changes	NA	Low
72	Enclave and Computing Environment	ECLO-2	Logon	NA	Medium
73	Enclave and Computing Environment	ECLP-1	Least Privilege	NA	High
74	Enclave and Computing Environment	ECML-1	Marking and Labeling	NA	High
76	Enclave and Computing Environment	ECND-2	Network Device Controls	NA	Medium
77	Enclave and Computing Environment	ECNK-1	Encryption for Need-To-Know	NA	Medium
79	Enclave and Computing Environment	ECPA-1	Privileged Account Control	NA	High
82	Enclave and Computing Environment	ECRG-1	Audit Reduction and Report Generation	NA	Low
83	Enclave and Computing Environment	ECRR-1	Audit Record Retention	NA	Medium
84	Enclave and Computing Environment	ECSC-1	Security Configuration Compliance	NC	High
85	Enclave and Computing Environment	ECSD-2	Software Development Change Controls	NA	High

Scorecard / DSN / Firewall / IA Checklist / IDS / Net Policy / Router / VTC / Calculations

Ready

DISA
A Combat Support Agency

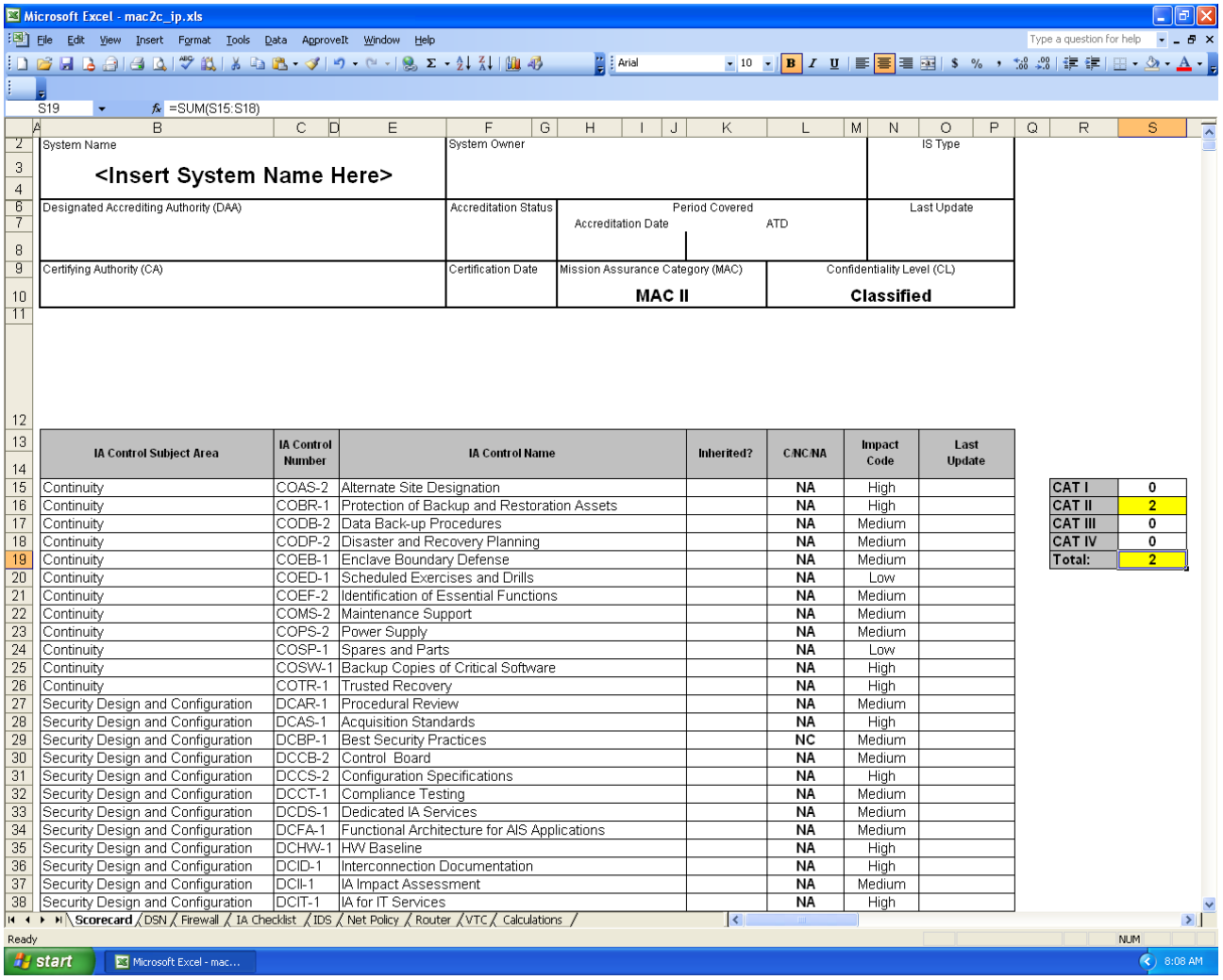
Four “NC”, Two CAT IIs

- **Remember, we have entered only two vulnerabilities into the Scorecard Matrix (V0017681 & V0017600).**
- **You can see in the next slide that each vulnerability is counted only once in the severity category table on the Scorecard page.**
- **Thus, even though four IA controls have failed (PRTN-1, IAIA-2, ECSC-1, & DCBP-1), the severity category table only shows 2 vulnerabilities, and they are both CAT II.**

DISA

A Combat Support Agency

Two CAT IIs



Microsoft Excel - mac2c_ip.xls

File Edit View Insert Format Tools Data ApproveIt Window Help

S19 =SUM(S15:S18)

System Name	System Owner	IS Type
<Insert System Name Here>		

Designated Accrediting Authority (DAA)	Accreditation Status	Period Covered: Accreditation Date	Period Covered: ATD	Last Update

Certifying Authority (CA)	Certification Date	Mission Assurance Category (MAC)	Confidentiality Level (CL)
		MAC II	Classified

IA Control Subject Area	IA Control Number	IA Control Name	Inherited?	C/NC/NA	Impact Code	Last Update
Continuity	COAS-2	Alternate Site Designation		NA	High	
Continuity	COBR-1	Protection of Backup and Restoration Assets		NA	High	
Continuity	CODB-2	Data Back-up Procedures		NA	Medium	
Continuity	CODP-2	Disaster and Recovery Planning		NA	Medium	
Continuity	COEB-1	Enclave Boundary Defense		NA	Medium	
Continuity	COED-1	Scheduled Exercises and Drills		NA	Low	
Continuity	COEF-2	Identification of Essential Functions		NA	Medium	
Continuity	COMS-2	Maintenance Support		NA	Medium	
Continuity	COPS-2	Power Supply		NA	Medium	
Continuity	COSP-1	Spares and Parts		NA	Low	
Continuity	COSW-1	Backup Copies of Critical Software		NA	High	
Continuity	COTR-1	Trusted Recovery		NA	High	
Security Design and Configuration	DCAR-1	Procedural Review		NA	Medium	
Security Design and Configuration	DCAS-1	Acquisition Standards		NA	High	
Security Design and Configuration	DCBP-1	Best Security Practices		NC	Medium	
Security Design and Configuration	DCCB-2	Control Board		NA	Medium	
Security Design and Configuration	DCCS-2	Configuration Specifications		NA	High	
Security Design and Configuration	DCCT-1	Compliance Testing		NA	Medium	
Security Design and Configuration	DCDS-1	Dedicated IA Services		NA	Medium	
Security Design and Configuration	DCFA-1	Functional Architecture for AIS Applications		NA	Medium	
Security Design and Configuration	DCHW-1	HW Baseline		NA	High	
Security Design and Configuration	DCID-1	Interconnection Documentation		NA	High	
Security Design and Configuration	DCII-1	IA Impact Assessment		NA	Medium	
Security Design and Configuration	DCIT-1	IA for IT Services		NA	High	

CAT I	0
CAT II	2
CAT III	0
CAT IV	0
Total:	2

Scorecard / DSN / Firewall / IA Checklist / IDS / Net Policy / Router / VTC / Calculations

Ready NUM

start Microsoft Excel - mac... 8:08 AM

DISA
A Combat Support Agency

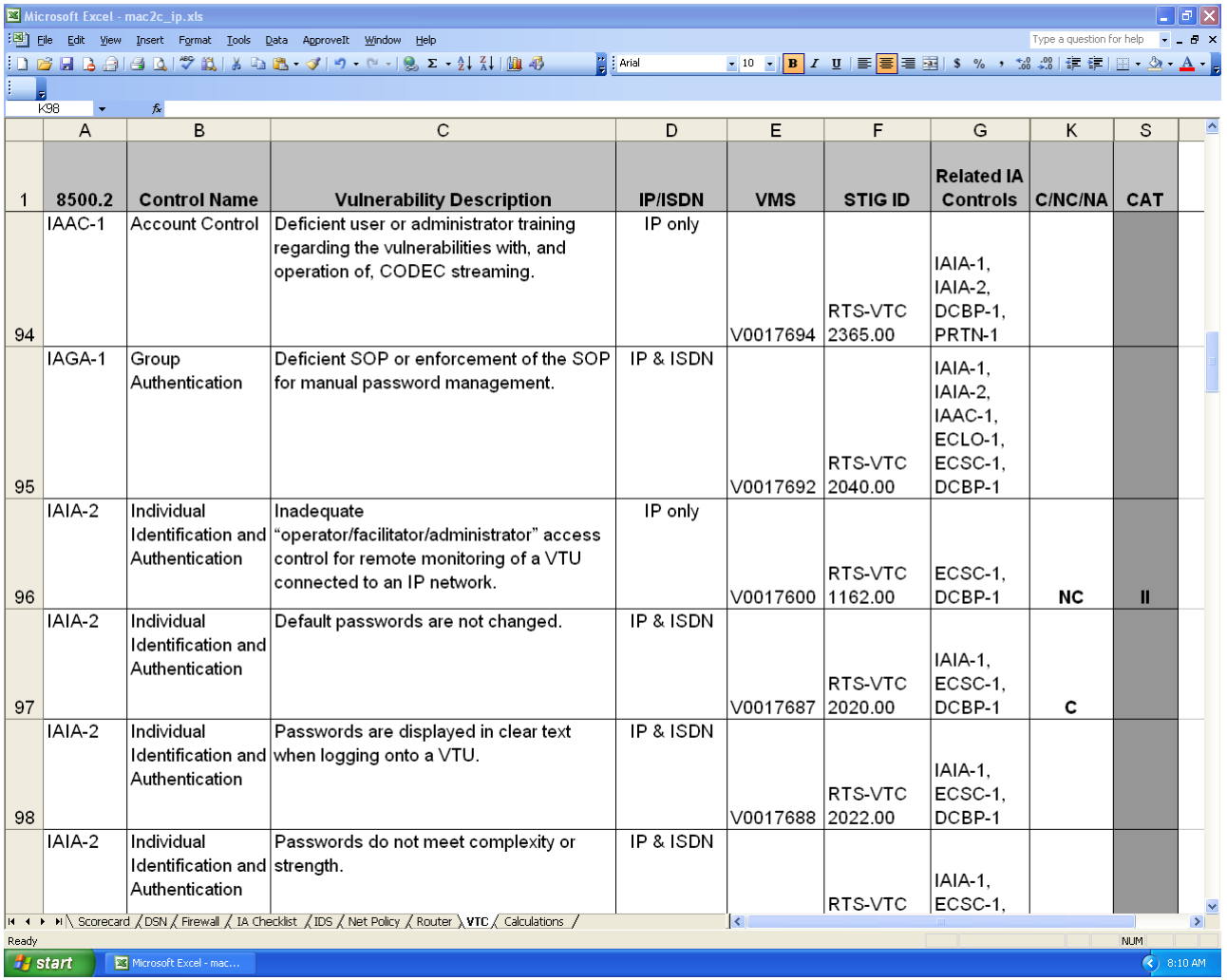
Back to IAIA-2

- Now let's go back to IA control IAIA-2 on the VTC spreadsheet.
- Notice that there is more than one STIG vulnerability related to IAIA-2.
- What happens if one IAIA-2 vulnerability fails, but another one passes?
- In the C/NC/NA column, type "C" for "Compliant," and then press "Enter."

No Severity Category

A Combat Support Agency

- **Notice that no severity category appears.**



Microsoft Excel - mac2c_ip.xls

	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
94	IAAC-1	Account Control	Deficient user or administrator training regarding the vulnerabilities with, and operation of, CODEC streaming.	IP only	V0017694	RTS-VTC 2365.00	IAIA-1, IAIA-2, DCBP-1, PRTN-1		
95	IAGA-1	Group Authentication	Deficient SOP or enforcement of the SOP for manual password management.	IP & ISDN	V0017692	RTS-VTC 2040.00	IAIA-1, IAIA-2, IAAC-1, ECLO-1, ECSC-1, DCBP-1		
96	IAIA-2	Individual Identification and Authentication	Inadequate "operator/facilitator/administrator" access control for remote monitoring of a VTU connected to an IP network.	IP only	V0017600	RTS-VTC 1162.00	ECSC-1, DCBP-1	NC	II
97	IAIA-2	Individual Identification and Authentication	Default passwords are not changed.	IP & ISDN	V0017687	RTS-VTC 2020.00	IAIA-1, ECSC-1, DCBP-1	C	
98	IAIA-2	Individual Identification and Authentication	Passwords are displayed in clear text when logging onto a VTU.	IP & ISDN	V0017688	RTS-VTC 2022.00	IAIA-1, ECSC-1, DCBP-1		
	IAIA-2	Individual Identification and Authentication	Passwords do not meet complexity or strength.	IP & ISDN		RTS-VTC	IAIA-1, ECSC-1,		

DISA

A Combat Support Agency

IAIA-2 Still "NC"

- **Also notice that IAIA-2 is still "NC" in the Scorecard.**

Microsoft Excel - mac2c_ip.xls

File Edit View Insert Format Tools Data ApproveIt Window Help

L96 =Calculations!J83

	B	C	E	L	M	N
85	Enclave and Computing Environmen	ECSD-2	Software Development Change Controls	NA	High	
86	Enclave and Computing Environmen	ECTB-1	Audit Trail Backup	NA	Medium	
87	Enclave and Computing Environmen	ECTC-1	Tempest Controls	NA	High	
88	Enclave and Computing Environmen	ECTM-2	Transmission Integrity Controls	NA	Medium	
89	Enclave and Computing Environmen	ECTP-1	Audit Trail Protection	NA	Medium	
90	Enclave and Computing Environmen	ECVI-1	Voice over IP	NA	Medium	
91	Enclave and Computing Environmen	ECVP-1	Virus Protection	NA	High	
92	Enclave and Computing Environmen	ECWM-1	Warning Message	NA	Low	
93	Enclave and Computing Environmen	ECWN-1	Wireless Computing and Networking	NA	High	
94	Enclave and Computing Environmen	IAAC-1	Account Control	NA	High	
95	Identification and Authentication	IAGA-1	Group Identification and Authentication	NA	Medium	
96	Identification and Authentication	IAIA-2	Individual Identification and Authentication	NC	High	
97	Identification and Authentication	IAKM-2	Key Management	NA	Medium	
98	Identification and Authentication	IAKM-3	Key Management	NA	Medium	
99	Identification and Authentication	IATS-2	Token and Certificate Standards	NA	Medium	
100	Physical and Environmental	PECF-2	Access to Computing Facilities	NA	High	
101	Physical and Environmental	PECS-2	Clearing and Sanitizing	NA	High	
102	Physical and Environmental	PEDD-1	Destruction	NA	High	
103	Physical and Environmental	PEDI-1	Data Interception	NA	High	
104	Physical and Environmental	PEEL-2	Emergency Lighting	NA	Medium	
105	Physical and Environmental	PEFD-2	Fire Detection	NA	High	
106	Physical and Environmental	PEFI-1	Fire Inspection	NA	Medium	
107	Physical and Environmental	PEFS-2	Fire Suppression System	NA	High	
108	Physical and Environmental	PEHC-2	Humidity Controls	NA	Medium	
109	Physical and Environmental	PEMS-1	Master Power Switch	NA	High	
110	Physical and Environmental	PEPF-2	Physical Protection of Facilities	NA	High	
111	Physical and Environmental	PEPS-1	Physical Security Testing	NA	Low	
112	Physical and Environmental	PESL-1	Screen Lock	NA	Medium	
113	Physical and Environmental	PESP-1	Workplace Security Procedures	NA	Medium	
114	Physical and Environmental	PESS-1	Storage	NA	High	
115	Physical and Environmental	PETC-2	Temperature Controls	NA	Medium	
116	Physical and Environmental	PETN-1	Environmental Control Training	NA	Low	
117	Physical and Environmental	PEVC-1	Visitor Control to Computing Facilities	NA	High	
118	Physical and Environmental	PEVR-1	Voltage Regulators	NA	High	
119	Personnel	PRAS-2	Access to Information	NA	High	

Scorecard / DSN / Firewall / IA Checklist / IDS / Net Policy / Router / VTC / Calculations /

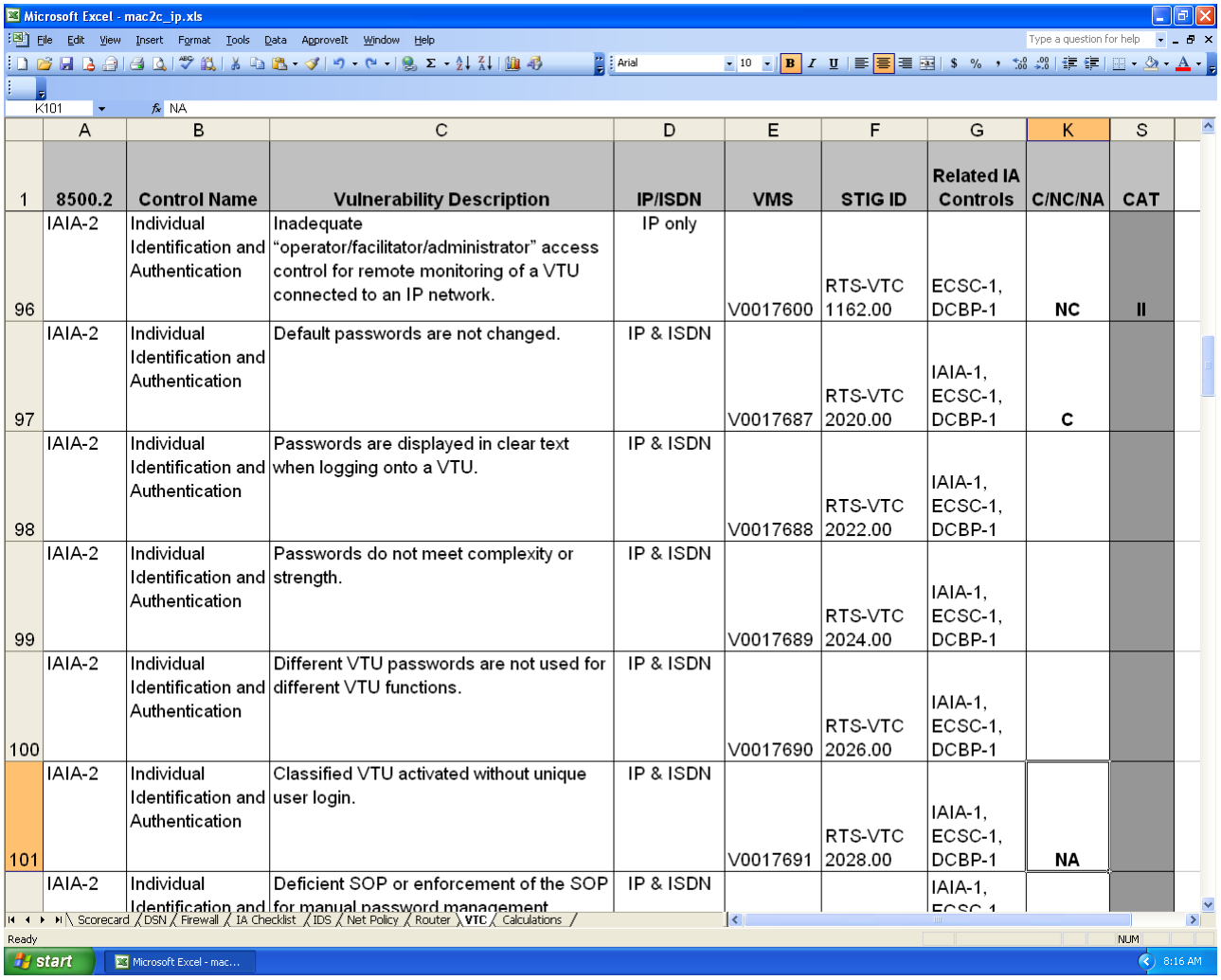
Ready NUM

start Microsoft Excel - mac... SM Shots - Microsoft ... 8:14 AM

"NA" & No Severity Category

A Combat Support Agency

- **Now go back to IAIA-2 in the VTC spreadsheet, type "NA," and then press "Enter." Notice that no severity category appears.**



	A	B	C	D	E	F	G	K	S
1	8500.2	Control Name	Vulnerability Description	IP/ISDN	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT
96	IAIA-2	Individual Identification and Authentication	Inadequate "operator/facilitator/administrator" access control for remote monitoring of a VTU connected to an IP network.	IP only	V0017600	RTS-VTC 1162.00	ECSC-1, DCBP-1	NC	II
97	IAIA-2	Individual Identification and Authentication	Default passwords are not changed.	IP & ISDN	V0017687	RTS-VTC 2020.00	IAIA-1, ECSC-1, DCBP-1	C	
98	IAIA-2	Individual Identification and Authentication	Passwords are displayed in clear text when logging onto a VTU.	IP & ISDN	V0017688	RTS-VTC 2022.00	IAIA-1, ECSC-1, DCBP-1		
99	IAIA-2	Individual Identification and Authentication	Passwords do not meet complexity or strength.	IP & ISDN	V0017689	RTS-VTC 2024.00	IAIA-1, ECSC-1, DCBP-1		
100	IAIA-2	Individual Identification and Authentication	Different VTU passwords are not used for different VTU functions.	IP & ISDN	V0017690	RTS-VTC 2026.00	IAIA-1, ECSC-1, DCBP-1		
101	IAIA-2	Individual Identification and Authentication	Classified VTU activated without unique user login.	IP & ISDN	V0017691	RTS-VTC 2028.00	IAIA-1, ECSC-1, DCBP-1	NA	
	IAIA-2	Individual Identification and	Deficient SOP or enforcement of the SOP for manual password management	IP & ISDN			IAIA-1,		

DISA

A Combat Support Agency

IAIA-2 Still "NC"

- **Also notice that IAIA-2 is still "NC" on the Scorecard.**

Microsoft Excel - mac2c_ip.xls

File Edit View Insert Format Tools Data ApproveIt Window Help

L96 =CalculationsU83

	B	C	E	L	M	N
85	Enclave and Computing Environmen	ECSD-2	Software Development Change Controls	NA	High	
86	Enclave and Computing Environmen	ECTB-1	Audit Trail Backup	NA	Medium	
87	Enclave and Computing Environmen	ECTC-1	Tempest Controls	NA	High	
88	Enclave and Computing Environmen	ECTM-2	Transmission Integrity Controls	NA	Medium	
89	Enclave and Computing Environmen	ECTP-1	Audit Trail Protection	NA	Medium	
90	Enclave and Computing Environmen	ECVI-1	Voice over IP	NA	Medium	
91	Enclave and Computing Environmen	ECVP-1	Virus Protection	NA	High	
92	Enclave and Computing Environmen	ECWM-1	Warning Message	NA	Low	
93	Enclave and Computing Environmen	ECWN-1	Wireless Computing and Networking	NA	High	
94	Enclave and Computing Environmen	IAAC-1	Account Control	NA	High	
95	Identification and Authentication	IAGA-1	Group Identification and Authentication	NA	Medium	
96	Identification and Authentication	IAIA-2	Individual Identification and Authentication	NC	High	
97	Identification and Authentication	IAKM-2	Key Management	NA	Medium	
98	Identification and Authentication	IAKM-3	Key Management	NA	Medium	
99	Identification and Authentication	IATS-2	Token and Certificate Standards	NA	Medium	
100	Physical and Environmental	PECF-2	Access to Computing Facilities	NA	High	
101	Physical and Environmental	PECS-2	Clearing and Sanitizing	NA	High	
102	Physical and Environmental	PEDD-1	Destruction	NA	High	
103	Physical and Environmental	PEDI-1	Data Interception	NA	High	
104	Physical and Environmental	PEEL-2	Emergency Lighting	NA	Medium	
105	Physical and Environmental	PEFD-2	Fire Detection	NA	High	
106	Physical and Environmental	PEFI-1	Fire Inspection	NA	Medium	
107	Physical and Environmental	PEFS-2	Fire Suppression System	NA	High	
108	Physical and Environmental	PEHC-2	Humidity Controls	NA	Medium	
109	Physical and Environmental	PEMS-1	Master Power Switch	NA	High	
110	Physical and Environmental	PEPF-2	Physical Protection of Facilities	NA	High	
111	Physical and Environmental	PEPS-1	Physical Security Testing	NA	Low	
112	Physical and Environmental	PESL-1	Screen Lock	NA	Medium	
113	Physical and Environmental	PESP-1	Workplace Security Procedures	NA	Medium	
114	Physical and Environmental	PESS-1	Storage	NA	High	
115	Physical and Environmental	PETC-2	Temperature Controls	NA	Medium	
116	Physical and Environmental	PETN-1	Environmental Control Training	NA	Low	
117	Physical and Environmental	PEVC-1	Visitor Control to Computing Facilities	NA	High	
118	Physical and Environmental	PEVR-1	Voltage Regulators	NA	High	
119	Personnel	PRAS-2	Access to Information	NA	High	

Scorecard / DSN / Firewall / IA Checklist / IDS / Net Policy / Router / VTC / Calculations

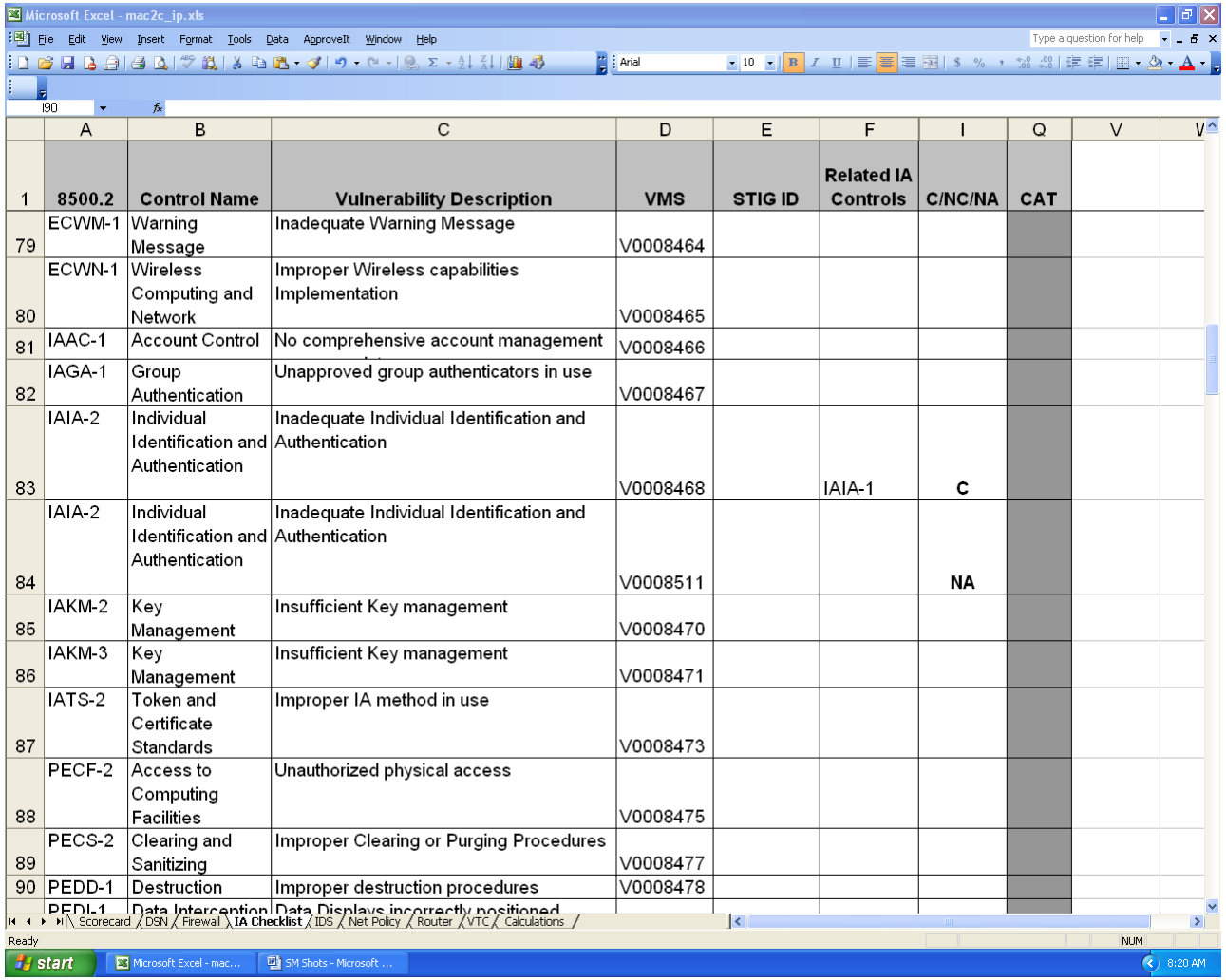
Ready NUM

start Microsoft Excel - mac... 8:18 AM

IA Checklist Spreadsheet

A Combat Support Agency

- **Now let's go to IAIA-2 in the IA Checklist spreadsheet. For fun, mark the two IAIA-2 vulnerabilities as seen below.**



Microsoft Excel - mac2c_ip.xls

	A	B	C	D	E	F	I	Q	V
1	8500.2	Control Name	Vulnerability Description	VMS	STIG ID	Related IA Controls	C/NC/NA	CAT	
79	ECWM-1	Warning Message	Inadequate Warning Message	V0008464					
80	ECWN-1	Wireless Computing and Network	Improper Wireless capabilities Implementation	V0008465					
81	IAAC-1	Account Control	No comprehensive account management	V0008466					
82	IAGA-1	Group Authentication	Unapproved group authenticators in use	V0008467					
83	IAIA-2	Individual Identification and Authentication	Inadequate Individual Identification and Authentication	V0008468		IAIA-1	C		
84	IAIA-2	Individual Identification and Authentication	Inadequate Individual Identification and Authentication	V0008511			NA		
85	IAKM-2	Key Management	Insufficient Key management	V0008470					
86	IAKM-3	Key Management	Insufficient Key management	V0008471					
87	IATS-2	Token and Certificate Standards	Improper IA method in use	V0008473					
88	PECF-2	Access to Computing Facilities	Unauthorized physical access	V0008475					
89	PECS-2	Clearing and Sanitizing	Improper Clearing or Purging Procedures	V0008477					
90	PEDD-1	Destruction	Improper destruction procedures	V0008478					
	PEDI-1		Data Interception Data Displays incorrectly positioned						

Scorecard | DSN | Firewall | IA Checklist | IDS | Net Policy | Router | VTC | Calculations

Ready

DISA
A Combat Support Agency

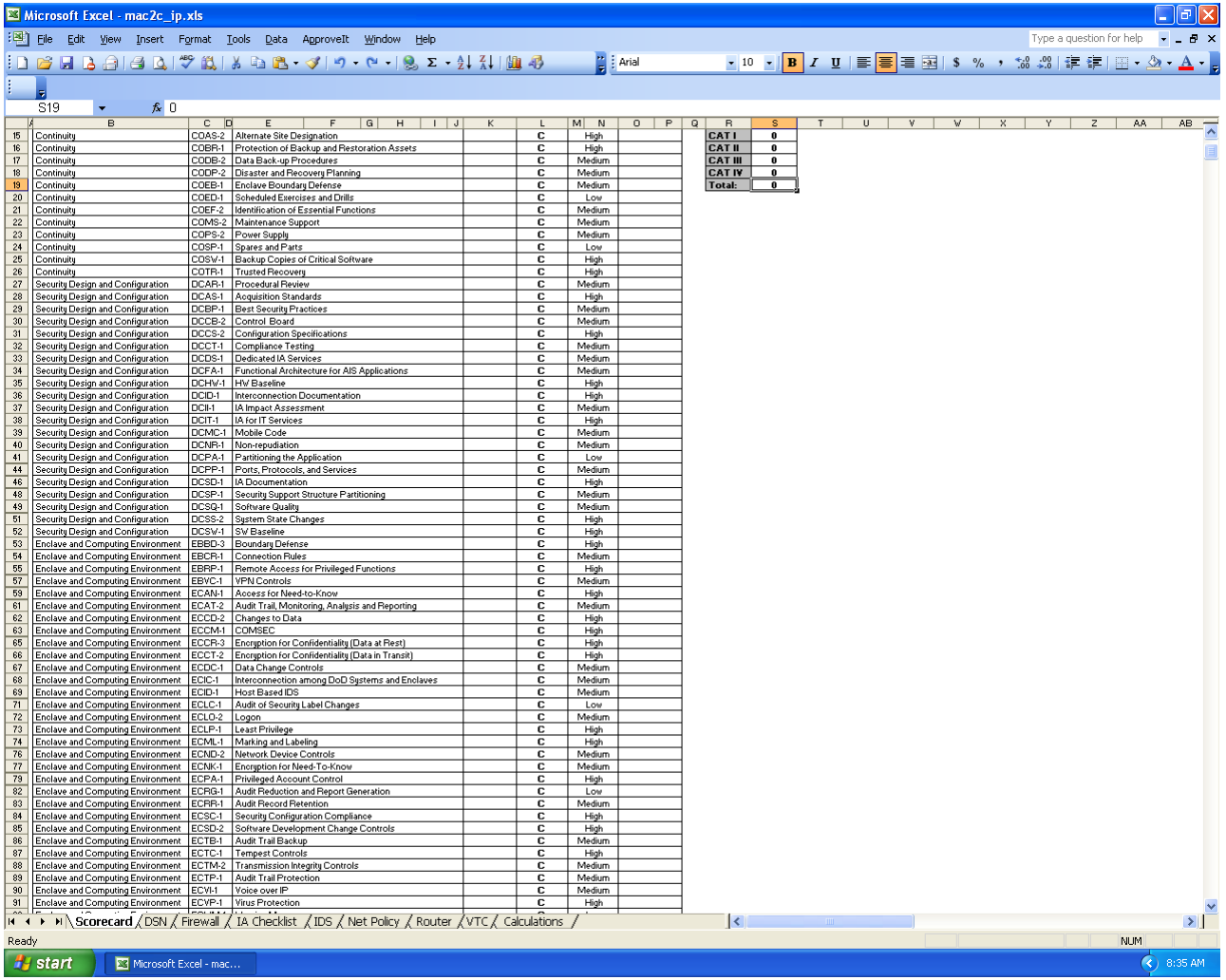
IAIA-2 Still "NC" in Scorecard

- **Despite what we've entered in the IA Checklist spreadsheet, because an IAIA-2 vulnerability failed in the VTC spreadsheet, IAIA-2 is still "NC" in the Scorecard.**
- **Even if all IAIA-2 vulnerabilities were "C" or "NA" except for one "NC", IAIA-2 would be "NC" on the Scorecard.**

The Final Goal

A Combat Support Agency

- **Once everything in your information system is compliant, your Scorecard will look like the one below, and your DAA will most likely give you an ATO.**



DISA
A Combat Support Agency

References

- **VTF DIACAP Scorecard Matrix**
  - **http://www.disa.mil/disnvtc/scorecard.htm**
- **For current and future ISDN & IP VTF customers: Everything you need for the VTF DIACAP Process is available at the VTF DIACAP Web Site:**
  - **http://www.disa.mil/disnvtc/diacap.htm**
- **DISA STIG Security Checklists are available from:**
  - **http://iase.disa.mil/stigs/checklist/index.html**
- **DISA STIGs are available from:**
  - **http://iase.disa.mil/stigs/index.html**
- **If you still have questions, contact the DISN Customer Contact Center (DCCC):**
  - **Commercial (614) 692-4790, option 4**
  - **Toll Free Commercial (800) 554-DISN (3476), option 4**
  - **DSN (312) 850-4790, option 4**
  - **Global DSN (510) 376-3222, option 4**
  - **DCCC@csd.disa.mil**

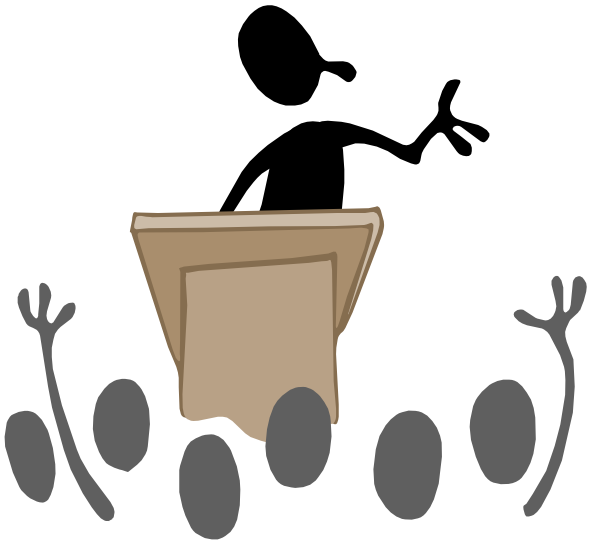
DISA
A Combat Support Agency

More References

- **DoD DIACAP Policies**
  - **Department of Defense Instruction (DoDI) 8510.01p, Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP): http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf**
  - **DoDI 8500.2, Information Assurance (IA) Implementation: http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf**
  - **Department of Defense Directive (DoDD) 8500.01, Information Assurance: http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf**
- **According to DoDI 8510.01p, DoD Information Assurance Certification and Accreditation Process (DIACAP), Section 6.3.2.2, DIACAP IA Control Validation Procedures are maintained through the DIACAP CCM and published in the DIACAP Knowledge Service (KS) (https://diacap.iaportal.navy.mil/).**

DISA
A Combat Support Agency

Questions?



www.disa.mil